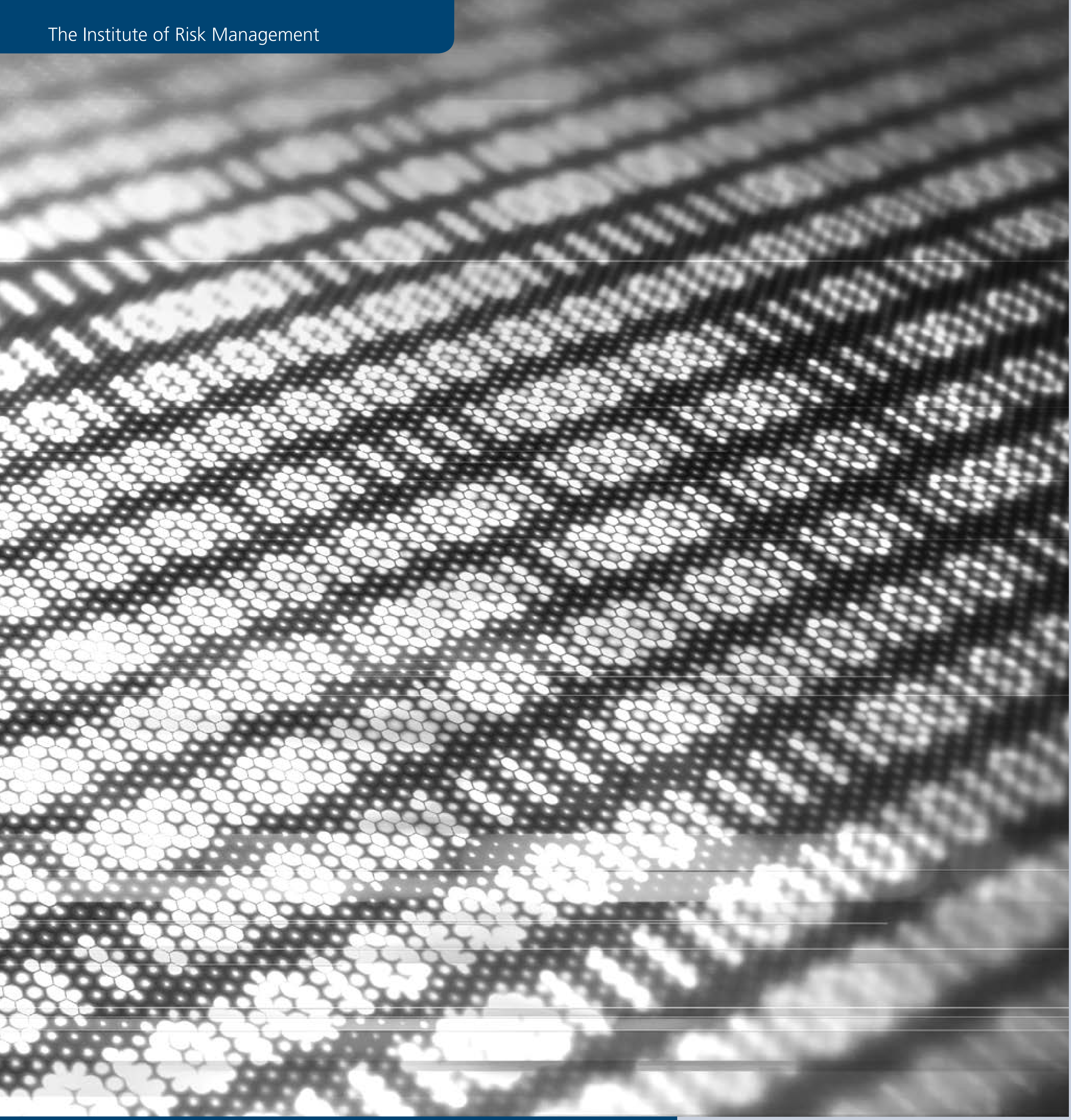
The Institute of Risk Management



Cyber Risk

Resources for Practitioners

CGI
Experience the commitment®

irm
Leading the risk profession

Leading the risk profession

The Institute of Risk Management (IRM) is the world's leading enterprise-wide risk management education Institute. We are independent, well-respected advocates of the risk profession, owned by our members who are practising risk professionals. IRM passionately believes in the importance of risk management and that investment in education and continuing professional development leads to more effective risk management.

We provide qualifications, short courses and events at a range of levels from introductory to expert. IRM supports its members and the wider risk community by providing the skills and tools needed to put theory into practice in order to deal with the demands of a constantly changing, sophisticated and challenging business environment.

We operate internationally with members and students in over 100 countries, drawn from all risk-related disciplines and a wide range of industries in the private, third and public sectors.

A not-for profit organisation, IRM reinvests any surplus from its activities in the development of international qualifications, short courses and events.

Experience the commitment®

Founded in 1976, CGI is a global IT and business process services provider delivering high-quality business consulting, systems integration and outsourcing services. With 68,000 professionals in 40 countries, CGI has an industry-leading track record of on-time, on-budget projects, whilst aligning our teams with clients' business strategies to achieve top-to-bottom line results. We have over 1,200 Cyber Security experts across the world who work closely with international security associations and standards bodies. We are one of a few providers worldwide with three accredited security certification facilities in the UK, the U.S. and Canada. Our nine Security Operations Centres continuously identify and deploy the best solutions to maintain a state-of-the-art infrastructure, handling over 70 million cyber events every day.

IRM does not necessarily endorse the views expressed or products described by individual authors within this document.

Our supporters

afm association of financial mutuals

alarm THE PUBLIC RISK MANAGEMENT ASSOCIATION

bci Business Continuity Institute

CIPFA

CGMA Chartered Global Management Accountant™

Powered by AICPA® | CIMA

CPNI Centre for the Protection of National Infrastructure

GCHQ

IET The Institution of Engineering and Technology

Built Environment

Chartered Institute of Internal Auditors

Foreword

I frequently say that the role of risk management is to be the disruptive intelligence that pierces the 'perfect place arrogance' so often encountered in organisations of all types. Our professional inclination to be upbeat and optimistic, together with significant personal and organisational investment in how things are, can lead to us being slow to react, or even wilfully blind, to major shifts in the risk landscape and our capabilities for dealing with them. At the same time, corporate governance developments around the world are placing explicit responsibilities on boards to ensure that they understand and manage their risk exposures.

Cyber risk is one such development. Over the past twenty years our working and personal lives have been transformed by these of technology. We can do things now to access and organise information, and to communicate with each other, that we could not conceive of in the last century. The pace of these developments shows no sign of abating. Technology has brought us huge benefits, but it also poses risks that need to be understood and managed. But while the risks might seem new, the ways of dealing with them are now well established. The IRM has worked to develop the profession of risk management, providing education, training and practical guidance to help organisations approach their risks in a systematic and effective way, from the board down to the shop floor.

This document presents the work undertaken by IRM's Risk in Information Systems and E-business (RISE) special interest group (SIG). It also incorporates ideas discussed at a series of round table events organised by IRM in partnership with BAE Systems Applied Intelligence. It is relevant for all professionals, particularly for those working at board level. It is not a technical document about computers and networks (there are plenty of those elsewhere). It is a document about risk management in the context of cyber risk, which we think is breaking new ground. There is also a shorter document summarising the key messages, particularly those of relevance at board level, which is available for free download from the IRM website.

As with all our thought leadership work, we are gathering together risk experts to look at fast-moving areas where practice is still being developed. We don't therefore think that what we have written here will be the last word on the subject – we expect to see new ideas and practices emerging and welcome comments. I am grateful to the RISE SIG, and particularly to its leaders Alastair Allison, David Canham, Matt Hillyer and Dan Roberts, for the enormous amount of work they have done to bring these documents together. I would also like to thank the wider international group of practitioners, experts and associations that the SIG has brought together to produce, contribute to and comment upon this work. Thanks are also due to our sponsors CGI who have made possible the design and print of these documents as well as contributing to the content. As a not-for-profit organisation such support is invaluable in helping us maximise our investment in the development and delivery of world class risk management education and professional development.

Richard Anderson, Chairman,
Institute of Risk Management

Foreword

Loss of corporate data, intellectual property or customers' financial details – or at worst sometimes all three.

Every day the media report another organisation which has been the victim of a cyber-attack. Usually it's the loss of corporate data, intellectual property or customers' financial details – or at worst sometimes all three. The consequences have varied from regulatory fines and reputational loss, through to the complete failure of a business and we know that cyber criminals can infiltrate an organisation's systems for days, or even years, without being detected. So businesses and government need to understand where the key cyber risks exist within their organisation, how to detect them and how to protect themselves from this rising threat, at the right level of cost. CGI is delighted to support this IRM Cyber Risk document of new approaches and best practice, and we look forward to engaging with their members to help them become confident that they are successfully managing their cyber security risk.

Tim Gregory, UK President, CGI

CGI
Experience the commitment®

Our project team

IRM would like to thank the following who have contributed in various ways towards the drafting and review of this guidance. Particular thanks are due to the authors of the individual chapters whose names, where possible, are shown at the start of each chapter:

Members of the IRM RISE Special Interest Group

Alastair Allison SIRM, Zurich Insurance Group

Angeliki Chatzilia, Crowe Horwath Global Risk Consulting

David Canham, MIRM, Aviva PLC

Matt Hillyer, CIRM, TNT UK Ltd

Dan Roberts, SIRM

Harvey Seale, CIRM, Nuffield Health

Matt Willsher, BAe Systems Applied Intelligence

Carolyn Williams MIRM, Institute of Risk Management

Also with thanks to:

GCHQ

Wendy Holt, CGI

Paul Hopkins, CGI

Tim Stapleton, Zurich North America

CPNI

Roger Garrini, Selex ES

Andy Coombs, HMRC

Jennifer Wood, HMRC

Julian Phillips, JP Risk

Dorothy Maseke, UAP Kenya

Jeff Miller, Zurich Insurance Group

> “Digital technologies, devices and media have brought us great benefits and offer enormous opportunities but their use also exposes us to significant risks.”

Contents

> "Those responsible for risk management within an organisation need to have understanding of the nature of the risks and of the practical tools and techniques that are available to address them."

Chapter 01:
Executive summary Cyber risk and risk management

Chapter 1: Executive Summary – cyber risk and risk management

Carolyn Williams

> Those responsible for risk management within an organisation need to have a full understanding of the nature of the risks and also of the practical tools and techniques that are available to address them.

Digital technologies, devices and media have brought us great benefits and offer enormous opportunities but their use also exposes us to significant risks. The media regularly present us with examples of organisations that have suffered financial loss and reputational damage as a result of problems arising from their information technology systems, whether this is as a result of human error, deliberate wrongdoing or some other form of technology systems failure. Governments and regulators are getting interested and are increasingly calling on businesses to take action to protect both their own assets and also the national infrastructure.

Those responsible for risk management within an organisation need to have a full understanding of the nature of the risks and also of the practical tools and techniques that are available to address them. Increasingly regulators and investors will expect organisations to provide information on their cyber exposures, which should be integrated with the organisation's overall consideration of risk exposure and appetite. Cyber risk is never a matter purely for the IT team (although they have an vital role) as human and organisational factors are just as important as having the right hardware and software.

This guidance document from the IRM's RISE (Risk in Information Systems and E-Business) Special Interest Group attempts to de-mystify the subject of cyber risk.

We are aiming to offer some independent and practical guidance for fellow risk professionals. Other professionals outside the IT field may also find it useful. Some of the group's findings and recommendations are based on research amongst IRM members around the world. The document is intended primarily for risk professionals, from all types of organisation and in all locations, who are charged with ensuring that their own organisations are equipped to manage these risks, but there are also some important messages for the boards of organisations, where ultimate responsibility will lie. Effective governance arrangements for cyber risk issues are needed and some further ideas on this are set out in chapter 5.

What do we mean by cyber risk?

By 'cyber risk' we mean any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems. Such a risk could materialise in the following ways:

- deliberate and unauthorised breaches of security to gain access to information systems for the purposes of espionage, extortion or embarrassment.
- unintentional or accidental breaches of security, which nevertheless may still constitute an exposure that needs to be addressed
- operational IT risks due to poor systems integrity or other factors

> Mobile devices have become part of our everyday life and the lines between business and personal use have become blurred, with implications for organisational security.

More about the nature of the threat can be found in chapters 2 and 3.

Organisations should not only be concerned with these things happening to them directly, but should also consider the effects should key companies in their supply chain or other parts of their extended enterprise be affected. (See chapter 7 for more about supply chain considerations).

Increasingly organisations will have suppliers in the new world of outsourced services and infrastructure that has been termed "the cloud". Use of the cloud in itself neither increases nor decreases the risk profile; an effectively controlled environment migrated to the cloud will, if the controls remain in place, continue to be effectively controlled, while a poorly controlled environment will be fraught with risk and threat regardless of the IT infrastructure choice. (For more information see chapter 8).

Cyber = Opportunity

New ways of working bring risks as well as opportunities. The business benefits offered to organisations by cloud computing, BYOD[1], social media and the 'internet of things' introduce a range of new risks as well as causing existing risks to evolve. Keeping track of this rapidly changing world while maintaining the flexibility to react to opportunities will be a challenge to organisations. (For more on information security risk and business opportunity management see chapter 6).

Social media has brought vast changes to our personal, social and business lives and has the potential to offer enormous opportunities or do great damage to organisations. An effective response plan to address this new environment will include the development of a social media policy, deployment of a multi-disciplinary team, effective training, careful handling of customer complaints and active monitoring of the organisation's own presence on the web. (For more about social media risk see chapter 10).

Mobile devices have become part of our everyday life and the lines between business and personal use have become blurred, with implications for organisational security. The RISE group's research found that over 90% of respondents said that their organisations allowed the use of personal mobile devices for business use, but only 37% exercised any controls in relation to the configuration and security of these devices. Risk managers will need to be creative to find a balance between what the user wants and what the organisation needs. (For more about mobile devices see chapter 9).

[1] Bring Your Own Device

The European Commission estimates that more than one million people worldwide are the victims of cyber crime every day.

"It will never happen to us"

Because the risks arising from cyber activities, particularly the use of the internet, are relatively new, most organisations do not have a lot of experience in understanding or dealing with them. But the message coming to us from government and from specialist agencies is that no-one is immune. The European Commission estimates that more than one million people worldwide are the victims of cyber crime every day[2]. All types and sizes of organisations are potentially affected, not just financial services firms, defence organisations and high profile names.

According to the 2013 Annual Study: Global Cost of a Data Breach, conducted by the Ponemon Institute, the average cost of a data breach to an organisation in 2013 ranged from $1.1m in India to $5.4m in the US.

Small businesses are not immune to cyber risks – there is growing evidence that criminals are targeting the less protected organisations. Much of the advice given in this document, particularly that relating to basic precautions and controls, can be applied in a proportionate way in small businesses.

"So I'll go and buy some insurance"

Many of the risks of a security breach can be covered by insurance and this will form an important part of the cyber risk control programme (see chapter 14 for more information). Insurance cover can include the costs of:

- forensics investigations to determine the severity and scope of a breach
- notifying individuals that they have been affected by a breach
- operating a specialist call centre to deal with enquiries from those affected
- providing free credit and identity monitoring to reassure those affected
- hiring a PR firm to provide specialist advice
- legal defence costs, settlements and indemnity payments

Insurance is important but it doesn't cover everything. Organisations will incur the costs of reputational damage, loss of customers, stock devaluation, corrective measures, IT upgrade costs and devaluation of intellectual property, the cumulative costs of which can exceed the insurable loss many times over. In many cases it is the control environment and the cultural and behavioural issues that need to be understood and addressed (and invested in) in addition to technical security measures. A coherent and business wide risk-assessment programme to understand and minimise the risks before a breach occurs is required to address the iceberg impact of a cyber-loss (for more information see chapter 4).

[2] Strategic Risk Cyber Guide 2012

Some form of data breach, deliberate or accidental, is now considered inevitable for all organisations at some point.

Training and investment are vital

People – what Verizon[3] calls 'the carbon layer – can be a weak point but are also the organisation's main asset and defence. Investment in training programmes and communications campaigns can be very effective, particularly where account is taken of the organisation's risk culture and how this influences the transfer of what is learned into everyday activity in the workplace. (For more information see chapter 15 on investment and chapter 13 on learning and behaviour).

Basic precautions should not be taken for granted

It is absolutely crucial that organisations know what constitutes their data "crown jewels", be it customer data, credit card data, intellectual property or knowledge and have a clear understanding what value it brings to the organisation. According to Verizon, 99% of breaches involved techniques that were not considered highly difficult and the UK government security services maintain that about 80% of cyber attacks would be defeated by basic security controls.

Having identified the key data, organisations need to review the risks to determine potential motivations for an attack.

Managing an incident

Some form of data breach, deliberate or accidental, is now considered inevitable for all organisations at some point. It will happen, so a robust incident response procedure needs to be in place to minimise financial and reputational damage when a breach occurs. Risk professionals need to make sure that their processes can respond to a breach in a timely manner to protect the organisation's reputation as well as minimise any harm to clients and customers. (For more information see chapter 12).

Conclusion

The threats are pervasive and agile, of national and international concern and consequently, all organisations need to accurately assess the cyber risk on their organisation. We have looked at some of the key risks facing organisations and put together this document that aims to help risk professionals assess the risk by de-mystifying it. Stripped of the 'techie speak', cyber risk is just another sort of risk which should be properly dealt with within the organisation's risk management framework and processes. We aim to bring about a sense of perspective that will allow for an informed debate, free from the scaremongering. With the right approaches, organisations can face up to the risks and with simple controls, eradicate the majority of the threats, make cyber-crime more difficult to achieve and safely seize the huge opportunities that technology, cloud, social media and mobile devices can bring.

[3] 2013 Data Breach Investigations Report, Verizon

Questions the organisation should ask itself about cyber risk

Does our cyber-risk strategy support our wider strategic priorities?

Governance and assurance

- Do we have an effective enterprise risk management process in place and are cyber risks fully integrated into this process?
- Are we clear who is responsible for managing risks, can we identify who on the board is responsible, who explains the risks to them and on what information will decisions be made?
- Have we considered our risk appetite in relation to cyber risks, have we communicated this to all functions and do we know if our resources being deployed effectively? How would we know if inappropriate risk taking was taking place?
- Are we fully aware of the regulatory and legal exposure? What privacy and data security laws and regulations might the organisation be subject to? What are the implications for our investment decisions?
- Does our cyber-risk strategy support our wider strategic priorities? Does our risk mitigation facilitate and enable growth? Are our controls delaying or blocking progress and are we agile enough to exploit market opportunities?
- Do we invest sufficiently in cyber risk mitigation, including training, incident preparedness and assurance? How do we prioritise our investment?
- Does our culture support the necessary activities to manage this risk?
- Does our internal audit programme give us sufficient assurance in respect of our cyber risk management?

Understanding the risk

- What is the value of the information we hold (e.g. intellectual property, financial, strategic plans and other business critical information, customer/personal data)? What are our 'crown jewels' that need the most protection?
- What is the potential impact if this information is stolen or corrupted (e.g. reputational damage; damage to market value and share price; loss of competitive advantage and market share, direct liabilities to third parties affected, regulatory censure)?
- How much would it cost a third party to obtain this information and what could it be worth to them?
- What are our customers/clients' expectations of our cyber security?
- How many of our critical business functions are outsourced to third parties? Have we conducted due diligence on the cyber security risks across our extended enterprise and supply chain, including the use of cloud based services? How much private and sensitive information is shared with these third parties? What provisions are there in the contracts to deal with cyber risk?
- Are our systems engineered to the best levels of security? What could be improved?

Do our business continuity plans include cyber risk scenarios?

- Do we have an effective mobile device strategy? How do we control the use of personal devices for organisational business?
- Are we using social media in our organisation? How do we know what our employees, customers and the public are saying about us on social media? Do we have a social media strategy and could we manage a social media crisis?

Incident response

- How will we know if we are being or have been attacked?
- Do we have an incident response plan and have we tested it? Do we have arrangements to obtain specialist advice and services post-breach (e.g. customer help lines)?
- Who has the responsibility to declare a cyber risk incident?
- Do our business continuity plans include cyber risk scenarios?
- Might we have cover under our existing insurance policies for financial losses caused by cyber-risks? Are there any other risk transfer possibilities?
- Are we prepared to do a root cause analysis following a breach, particularly to identify human factors, and are we prepared to act on the findings?
- Could we defend our level of preparation in the aftermath of an attack?

Training

- Do we have an effective cyber risk training programme in place including reporting of breaches and subsequent actions?
- Are there initiatives in place to support learners after the training has taken place?
- Does our cyber risk training focus on the technology, the organisation or the individual?

Transforms from Entity to DTO.
item entity to convert
result of transformation DTO or <code>null</code>
IllegalArgumentException if the specified object is
IllegalArgumentException
Transforms from Entity list to DTO list.
@param items Entity list to convert
@return result of transformation DTO list o
@throws IllegalArgumentException if the s
Collection<V> transformToDto(Collection<K>
Transforms from DTO list to Entity list.
@param items DTO list to convert
@return result of transformation Entity list
Collection<K> transformFromDto(Collection<
transformFromDto(V item) throws IllegalArgumentException
Transforms from Entity list to DTO list.
@param items Entity list to convert
@return result of transformation DTO list or empty
@throws IllegalArgumentException if the
029
030
031
032
033
034
035
036
037
038
039

> “The threats are pervasive and agile, of national and international concern and consequently, all organisations need to accurately assess their cyber risk exposure.”

Chapter 02: Introduction

Chapter 2: Introduction

Alastair Allison CISM SIRM

Cyber crime challenges many of our traditional governance models.

The earliest "pyrates" recorded were the Sea Peoples in the 14th century BC who patrolled the lucrative trade routes around the Aegean and Mediterranean seas. Some historians have seen them as displaced Minoans following the destruction of their civilisation with the eruption of Thera (now Santorini), and the subsequent displacement of people throughout the Mediterranean. Nevertheless, the "pyrates" intercepted the trade for their own benefit. Roll forward to the modern, digital, trade routes where the majority of today's business is conducted.

Modern day predators now prowl these digital trade routes for their own benefit. Russian Alexandr Sergeyevich Bobnev, one of the top cyber criminals on the FBI's wanted list, was indicted in 2007 for his alleged participation in a money laundering scheme involving unauthorised access to the accounts of a major provider of investment services. He accessed compromised accounts and transferred funds to money mules in the United States – a cyber pirate perhaps. Where the Sea Peoples may have been "pyrates" simply to survive, their activities were geographically limited. Cyber pirates have no geographical borders and international law enforcement is simply not agile enough to keep up with them. Indeed, cyber crime challenges many of our traditional governance models. But what do we actually mean by "cyber crime"?

Cyber crime is the use of computer technologies to commit a crime. Cyberspace is defined as "the independent network of information technology infrastructures. It includes the internet, telecommunication networks, computer systems and embedded processors and controllers in various industries"[4].

Criminality will always follow the money. In the 19th Century in the UK, highwayman Dick Turpin was after the riches of the few. In the 20th Century criminals Jesse James and Ronnie Biggs blew up the money vaults and took stacks of cash. This digital age of the 21st Century is no different: Bobnev busted the digital vault for virtual cash. In all these cases, wealth was taken away from the rightful owner. But is this the only motivation of cyber criminals? According to the 2013 Verizon report, Cyber criminals fall into three distinct threat types: activists, criminals and spies. We add two further distinctive threat types; your own staff and your own systems.

- **Activists** are opportunistic in their approach and often use only basic methods but, unlike the criminals who may be financially motivated, their key aim may be to cause embarrassment or, in the case of "script kiddies"[5] they may simply want to see what they are capable of doing.

[4] As defined by The Democratic Governance Challenges of Cyber Security (DCAF) www.dcaf.ch

[5] In hacker culture a script kiddie or skiddie is an unskilled individual who uses scripts or programs developed by others to attack computer systems and networks and deface websites. It is generally assumed that script kiddies are juveniles who lack the ability to write sophisticated hacking programs or exploits on their own, and that their objective is to try to impress their friends or gain credit in computer-enthusiast communities. Wikipedia – accessed 7 Oct 13.

Cyber risk is pervasive and is not just about crime and stealing money, or assets to exchange for money.

- **Criminals** are motivated by financial gain and use increasingly high levels of sophistication during their attacks including blackmailing vulnerable staff members to steal data from their employer's organisation. There is a whole underground criminal marketplace of capabilities to perpetrate cyber crime including help desks, marketing services and trade fairs where anyone can buy anything from hacked passwords to virus scripts.
- **Spies** are state controlled and employ the most sophisticated techniques. They can target everything, from intellectual property for increased competitive advantage to nation state infrastructure in order to cause damage for political or warfare purposes.
- **Own staff** represent the insider threat – the hard to detect shadow operating within the secured perimeter. The macro and micro economic situation has threatened the livelihoods of many and there is increasing evidence that criminal gangs are targeting vulnerable staff in organisations to help steal valuable information. With insider assistance, these criminals are able to plant technologies within the organisation which enable them to carry out attacks on systems. We should also not forget the humble human error which, when compounded by poorly controlled and secured systems, has the capability of opening up opportunities for others to exploit. Even if you keep all your systems up to date with patches, and have an agile patching cycle, the weakest link will always be the person behind a keyboard!
- **Own systems**, often built over a number of years or grown in line with the business and mergers and acquisitions, these pose a significant threat type in their own right. Poorly supported and insecure operating systems, poor patching controls and a lack of investment in security all add up to making it easier for the active threat actors such as those shown above.

Whilst it is tempting to look at these threats in terms of our own organisations we must also review the impact across our extended enterprise, looking at our exposure should a supplier, partner or customers be compromised. Consequently, we must not lose sight of the fact that the cyber risk is pervasive and is not just about crime and stealing money, or assets to exchange for money, but also encompasses risks arising from other factors such as government espionage, hacktivism, script kiddies, system integrity etc. Further, we must bear in mind that it is not just the bigger businesses that are targets.

Experts have noted that companies may at times forgo investment in security since they have not been attacked before or because they mistakenly believe that they have nothing a cyber adversary would want"[6]. Smaller businesses also have an unsupported belief that they are immune from the threat. Small businesses are actually easier

[6] Bucci, SP, Rosenweig, P and Inserra D, 2013, A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace accessed on line at http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace on 8 April 2013

> It is absolutely crucial that organisations know what constitutes the data “crown jewels”.

63%	of small businesses were attacked by an unauthorised outsider in the last year (up from 41% a year ago)
23%	of small businesses were hit by denial-of-service attacks in the last year (up from 15% a year ago)
15%	of small businesses detected that outsiders had successfully penetrated their network in the last year (up from 7% a year ago)
9%	of small businesses know that outsiders have stolen their intellectual property or confidential data in the last year (up from 4% a year ago)

Small businesses used not to be a target, but are now reporting increasing attacks (UK BIS Information Security Breaches Report 2013).

targets and there is growing evidence of criminals going for the less protected organisations, exploiting multiple failures in technology, processes and people; indeed staff related incidents have risen sharply in small businesses. According to Verizon’s 2013 Data Breach Investigations Report (DBIR), 99 percent of breaches involved techniques that were not considered highly difficult. Most data breaches are successful because the criminals found an easy entry point and not because they employed some level of sophisticated attack. The BIS 2013 Information Security Breaches report highlights some very specific statistics for small businesses as shown above. At the end of the day no organisation is safe or immune.

But is it really all doom and gloom? Should we simply switch off the computers and go back to paper and typewriters like the Russian Government proposed to do in 2013? Not necessarily.

It is absolutely crucial that organisations know what constitutes the data “crown jewels” be it customer data, credit card data, intellectual property or knowledge. These organisations need to have a clear understanding of what value these “crown jewels” bring to the organisation.

Having identified the key data, organisations need to review the risks, based on the threat vectors described above to determine potential motivations for an attack and how intent someone might be in obtaining the data. This may lead to withdrawing the use of computers if the information is so sensitive and facing a real threat of discovery. However, for most commercial organisations, examining their operating environment across the extended enterprise is the next key stage to seeing what vulnerabilities exist. Whilst this research looks at some robust solutions that could help overcome some key risks, organisations have to consider their proportionality i.e. if the solutions are proportionate to both the risk they face and the size of the organisation.

100% security is expensive, intrusive and rarely achievable in this fast paced world that we live in. Consequently, organisations must be able to respond to incidents in an effective manner that protects the potential victims as much as possible. We are not suggesting surrender to the inevitable at the expense of preventing breaches in the first place. However, there needs to be a balance between risk efficient prevention and being ready to react when the need arises.

> The threats are pervasive and agile, of national and international concern and consequently, all organisations need to accurately assess their cyber risk exposure.

> Each organisation must identify the risks appropriate for them and prioritise them according to their established risk frameworks. They will also need to determine the appropriateness of the material to their organisation.

Today we live in an interconnected world with so much data that it is critical to exercise oversight of the information being transferred and shared between organisations in our complex supply chains. That level of interconnectedness was debated at the G20 Summit in Davos which drew attention to the reliance on web-based technologies and cyberspace to control our national infrastructure. Governments have realised the threat of cyber risk and it has appeared on some national strategic risk registers. Consequently, there are growing regulatory and legal demands being made on businesses to not only protect data but also the national infrastructure. The EU, UK, USA, Israel, China, Iran and Syria have all announced significant cyber capabilities being put in place with not all of them being for defence purposes. The EU has a proposed Cyber Security Directive on its books with an aim of increasing international law enforcement and data sharing in a bid to tackle these growing threats.

So, the threats are pervasive and agile, of national and international concern and consequently, all organisations need to accurately assess their cyber risk exposure. This is where the IRM Cyber Research comes in. In the first half of 2013 the IRM RISE SIG undertook a survey of several hundred IRM members and contacts around the world to assess their perceptions of cyber risk and their organisation's response to it. Based on the results of this work, we have looked at some of the key risks facing organisations and put together this document that aims to help risk managers assess the risk by de-mystifying it. Stripping it of the techie speak, we also aim to bring about a sense of perspective that will allow for an informed debate, free from the scaremongering. With the right approaches, organisations can face up to the risks and with simple controls, eradicate 85% of all threats. With the right approaches, we can look to seize the opportunities that cloud, social media and mobile devices can bring.

It is not appropriate for this document to provide all the scenarios, risk lists or a risk profile. It also does not aim to dive into the technical detail for the IT practitioners. This is because our own survey highlighted a gap in the risk manager's understanding of the cyber risk landscape and its borderless characteristic. Additionally, we specifically did not want to replicate the fact that there is a wealth of good material on technical controls and the lower level detail. Consequently, this research aims to de-mystify the cyber risk landscape and provide risk managers with the guidance to take an informed approach, for example when facilitating cyber risk workshops. Each organisation must identify the risks appropriate for them and prioritise them according to their established risk frameworks. They will also need to determine the appropriateness of the material to their organisation but this document covers the key themes and whilst not all the approaches are suitable for the small business, they are at least scaleable.

> “The threat to national security from cyber attacks is real and growing, whether from hacktivists, terrorists, cyber criminals, or hostile foreign states.“

Chapter 03:
The threat landscape

Chapter 3:
The threat landscape

Centre for the Protection of National Infrastructure (CPNI)

One major London listed company ... estimates that it incurred revenue losses of some £800m as a result of hostile state cyber-attack.

Cyberspace and the internet have revolutionised the way in which we communicate. This greater interconnectivity has provided enormous benefits for knowledge-based economies, enabling businesses to operate globally with greater speed and efficiency. But with such great opportunity comes sizeable risk, which must be managed. This chapter looks at how government and industry in the UK are working together to address this, helping protect essential services and safeguard our economic well-being.

The threat to national security from cyber attacks is real and growing, whether from hacktivists, terrorists, cyber criminals, or hostile foreign states. In his first public speech in October 2013 the new Director General of the UK Security Service MI5, Andrew Parker referred to the internet and related technologies as offering a world that is "better in so many ways, but better too for the terrorists". Cyberspace offers a largely anonymous and potentially very efficient means to achieve aims such as these. Governments and business alike need to be alive to the threat, understand what risks this poses for them and what measures can be put in place to manage them.

How big an impact are cyber-based threats having on the UK economy?

The scale of the problem was put into context in June 2012 by the former Director General of the Security Service MI5, Jonathan Evans who highlighted, "The Boards of all companies should consider the vulnerability of their own company to this threat as part of their normal corporate governance – and they should require their key advisors and suppliers to do the same. One major London listed company with which we have worked estimates that it incurred revenue losses of some £800m as a result of hostile state cyber-attack – not just through intellectual property loss but also from commercial disadvantage in contractual negotiations."

Espionage

In a BBC radio series earlier in the year, MI5's Head of Cyber referred to there being three certainties in life – "death, taxes and a foreign intelligence service on your system". He said that hostile foreign states are interested in a company's mergers and acquisitions activity, joint venture intentions and strategic direction over the next few years – that information would be valuable to that country's state owned enterprises.

93% of large corporations and 87% of small businesses had experienced a cyber breach in the past year.

Threats, extortion and denial of service attacks

Apart from the theft of sensitive business information, there is also the threat that cyber-based systems can be disrupted to prevent normal service. A Denial of Service (DoS) attack could prevent customers from accessing key websites, such as those for online banking. There is also the threat of disruption to critical industrial control systems such as supervisory control and data acquisition (SCADA). Almost all key industrial infrastructures and processes are managed using computers and communications networks. This includes the flow of gas and oil through pipes, the processing and distribution of water, the management of the electricity grid, the operation of chemical plants, and the signalling network for railways. This is why CPNI is helping operators to understand and mitigate vulnerabilities in these systems by funding research and working with international partners.

In 2013 the Channel 4 television drama, Blackout, illustrated a possible worst-case scenario of a cyber attack on the UK's National Grid system. Showing scenes of lawlessness and chaos within a few days of the power going down – with gridlocked traffic, looting, communications breakdowns and the government implementing its emergency response plan – Blackout received mixed reactions from viewers and opened an animated debate about whether such a scenario was possible. One cyber analyst said:

"It was a drama and it was interesting – albeit portraying the worst of a worst-case scenario. However, if it served to help raise awareness and if businesses are now taking things more seriously as a result of what was portrayed on screen, then it was useful."

What is Government doing?

National policy is led by the Office of Cyber Security & Information Assurance (OCSIA), which supports the Minister for the Cabinet Office and the National Security Council in determining priorities in relation to securing cyberspace. The unit provides strategic direction and coordinates the National Cyber Security Programme (now £860 million over 5 years) which is delivered by lead government departments and agencies such as the Home Office, Ministry of Defence, Government Communications Headquarters (GCHQ), the Security Service MI5, CPNI, the Foreign & Commonwealth Office (FCO) and the Department for Business, Innovation & Skills (BIS).

IT can only provide part of the solution.

The challenge for businesses

The challenge facing companies is understanding the magnitude of the threat and taking it seriously enough before real damage is done. The scale of the problem was put into context recently by figures from PwC's 2013 Information Security Breaches Survey showing that 93% of large corporations and 87% of small businesses had experienced a cyber breach in the past year. It is commonplace for boards of directors to see this as an IT issue since it is electronically stored information and systems that are targeted. What is not always considered are the wider implications for the competitiveness or long-term performance of the company.

Ensuring effective IT is only part of the solution; advancements in technology development move at pace and so does the threat. A control measure that may have been effective a year ago may now prove to be a vulnerability. Analysts are clear that businesses will need to regularly review their management of cyber risks. They believe the cyber threat needs to be taken as seriously as other major business issues like, for example, currency fluctuation or international law.

So what should industry be doing to manage cyber risks?

Ironically, one of the major ways of managing cyber risks is through appropriate sharing of technical information and data. A partnership between government and industry on information sharing helps to understand what cyber incidents are happening in the private sector and enables government to better understand and respond to threats.

One example is the UK Cyber-Security Information Sharing Partnership (CISP). CISP is a joint, collaborative initiative between industry and government to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact upon UK business. **www.cisp.org.uk**

But as previously described, IT can only provide part of the solution. The boards of all companies should consider the vulnerability of their own company to this threat as part of their normal corporate governance. According to GCHQ, CPNI, BIS and OCSIA (Cyber Security Guidance for Business), the key questions that company boards should routinely review include:

- Does the board appreciate the business benefits of effective enterprise risk management, and its role in managing emerging threats such as cyber-based threats?

- Does the organisation understand the value of the information it holds – its 'data crown jewels' (e.g. intellectual property, financial, strategic plans and other business critical information, customer/personal data)?
- What is the board's understanding of the potential impact if this information is stolen or corrupted (e.g. reputational damage; damage to market value and share price; loss of competitive advantage and market share)?

Companies benefit from managing risks across their organisations (and also into their wider 'extended enterprises' of suppliers, partners etc;) drawing effectively on senior management support, risk management policies and processes, a risk aware culture and the assessment of risks against objectives.

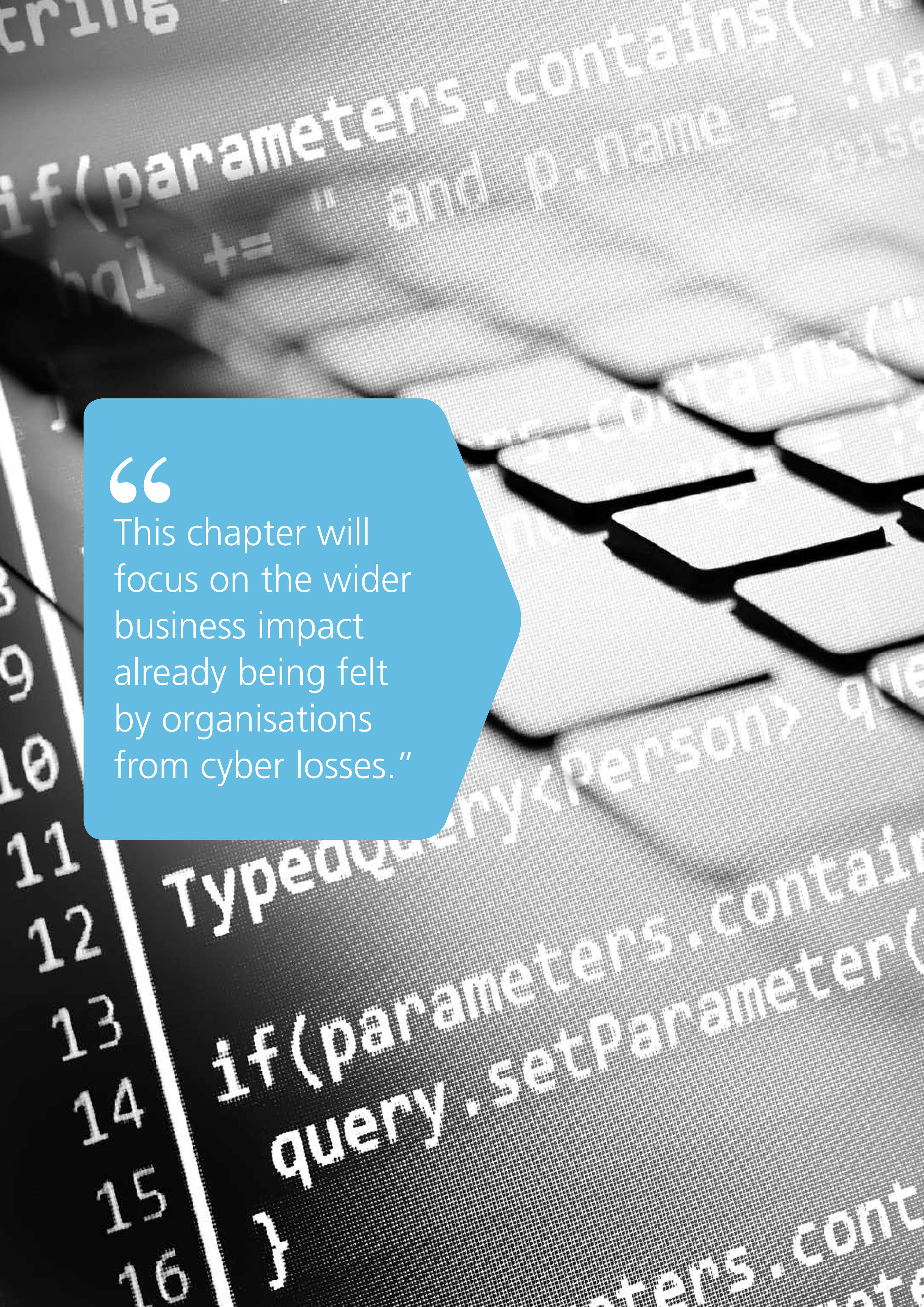
Information on both the potential threats and implementing risk management through corporate governance is explored in the 'Executive Companion' of Cyber Security Guidance for Business (referred to above). In addition, detailed guidance sheets are provided outlining the measures that can be taken to reduce information risk in ten key areas. The contents of both the 'Executive Companion' and the detailed guidance sheets can be used to support a board-level comprehensive risk management regime which can be effective in managing the organisation's information risks. **https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility**

What support is available?

Plenty of advice and guidance is available, for example on risk management, technical security measures and incident response services. Organisations also need to be prepared to address the overarching questions, and articulate their own understanding of the value and vulnerabilities of their business information.

The delivery of protective security advice to the national infrastructure and companies of national economic importance is undertaken by CPNI, who recommend that managing new and emerging threats such as those posed by cyberspace, should be at the heart of any organisation's corporate risk management strategy. For these companies CPNI (see **www.cpni.gov.uk**) provides a range of support, training, and guidance documents to assist them to:

- understand security threats (terrorism, espionage and sabotage),
- determine their exposure (risk), and
- manage risks in line with their corporate appetite.



> “This chapter will focus on the wider business impact already being felt by organisations from cyber losses.”

Chapter 04:
The iceberg impact of a cyber loss

Chapter 4: The iceberg impact of a cyber loss

Matt Hillyer

> The much broader and deeper implications of a loss more rarely register with senior executives until they themselves are dealing with the fallout.

Introduction

As cyber risk continues to grow the financial implications of a cyber loss grow even faster. With the size of penalties set to increase significantly over the coming years, the subject of cyber risk will become an area of greater importance for executive boards. Indeed in July 2013 MI5 and GCHQ felt the need to jointly write to the FTSE Top 350 companies highlighting "that cyber attacks against UK companies are already causing significant damage to their reputations and revenues."

This chapter will focus on the wider business impact already being felt by organisations from cyber losses. The chapter will explore the size and types of impact incurred from current cyber incidents and highlight that the potential financial losses can significantly exceed the headline sums associated with the regulatory penalties.

The reality for businesses

All too often we see the news headlines describing:

"Organisation X fined €100,000 following an employee leaving a memory stick on the train."

This frequent highlighting of the simplicity of a breach occurring and the ease with which fines are handed out does raise the boardroom profile of cyber risk. However the much broader and deeper implications of a loss more rarely register with senior executives until they themselves are dealing with the fallout of an incident.

The 2010 study by the Ponemon Institute calculated the average organisational cost of a data breach to be $7,241,899 (€5,576,262). This clearly demonstrates, as suggested by the title of this chapter, that the true business cost of an incident is many factors greater than the headline grabbing fine.

From the IRM Cyber Risk Survey, conducted as part of the research behind this document, it was established that many risk professionals are unable to accurately quantify the impact of a breach, with 82% of respondents not knowing the financial cost of cyber loss incidents within their organisations.

However, as organisations begin to count the impact of the cyber loss the variety of costs attributed to the event can very quickly add up.

The range of the impact

The impact from cyber losses can be split into 2 key types; non-insurable and insurable:

Those areas deemed to be insurable are explored in more detail in Chapter 14 which covers cyber insurance.

The remainder of this chapter focuses on the non-insurable impact from a cyber loss.

Sources:
- Supply
- Chain
- Cloud
- Mobile
- Social
- Media

The Impact:
Non-Insurable
- Fines
- Reputational Damage
- Loss of Customers
- Loss of Employees
- Stock Devaluation

The Impact:
Insurable
- Crisis Management
- Forensics
- Investigation
- Customer Notification
- Business Interruption

Non insurable costs of an incident

This section explores a number of the non-insurable costs associated with a cyber loss but is not necessarily a fully exhaustive guide.

Fines

Fines are the easiest to quantify and the most frequently associated impact of a cyber loss. The powers to issue fines differ within different regions and organisations should be clear as to the regulations which apply to them in all the jurisdictions in which they operate.

Case Study – Brighton and Sussex NHS Trust

The trust was fined £325,000 – the largest fine by the ICO to date – for sensitive patient data being found on hard drives sold on eBay.

The trust was unsure how the drives could have been removed from the premises but admitted that the drives may not have been secured at all hours during which a contractor had access.

In the UK the Information Commissioners Office (ICO) is empowered to issue fines of up to £500,000 to organisations in breach of data protection laws which are frequently broken within cyber security events. Since it was given the powers to issue Civil Monetary Penalties in April 2010, the ICO has issued over £4.6m of fines against organisations.

The range in financial penalties varies significantly across the globe with some countries / jurisdictions yet to apply a structure of fines, to the courts ascertaining the costs of damages, right through to the fines awarded by the Brazil and Mexico authorities of over US$1.5m (€1.155m).

In general, many of the Western governments have well established legislation and high penalties of several hundred thousand Euros. See Appendix 1 of this chapter for details of maximum fines by country.

Fines are covered in further detail in the cyber insurance chapter.

Loss of intellectual property can have a devastating impact.

Reputational damage

It is often difficult to quantify the impact of damage to your organisation's reputation following a breach. It is an area where some insurance can provide an element of restorative cover – see the cyber insurance chapter – but generally organisations will have to monitor and assess the ongoing impact to their brand and reputation.

Loss of customers

The loss of customers is a likely consequence from a significant cyber loss. This may be due to the termination of a contract through breach of a service level agreement related to the loss or through negative publicity created from the incident. The longer term impact of a loss can also have a major effect on new customer acquisition. Indeed within certain sectors, including the public sector, financial services or healthcare, a significant loss may prevent your organisation from tendering for future opportunities

Loss of employees

As well as customers being lost by the negative publicity of a cyber loss, it is equally possible for your own employees to be affected. For employees within a highly professional environment, the association with an organisation which has suffered a significant breach may be viewed as damaging to long term career prospects.

Indeed following the high profile information security breach at HBGary, which highlighted significant issues in employee controls, employee turnover increased as individuals sought to protect their professional profiles.

Stock devaluation

Share price is certainly impacted in the immediate aftermath of a disclosure of a cyber loss often driven by the negative publicity which is associated with the breach. In conducting this research it has been difficult to find evidence of long term share price damage associated purely with a cyber loss. Indeed some research has suggested that the impact on share price is reducing as perhaps shareholders become less sensitive to breaches. A report published in the Journal of Computer Security in 2011 suggested that "with increased media reporting of information security breaches without apparent devastating effects on targeted corporations, investors lowered their assessment of the costs of such breaches".

It is safe to assume however that where the cyber loss has other significant impact in terms of major customer losses or highly punitive regulatory fines then the organisation's share price would suffer some negative effect.

Case Study – Sony Corporation

Following the theft of details for 77 million of its PlayStation Network customers in April 2011, Sony saw a continuing decline in its share price of around 24% in the months after the incident. However, despite the reported $150m cost of the incident to Sony, over the longer term their share price has recovered. In addition there is no doubt that the incident certainly created some brand damage although the impact of this may have been lessened by the loyalty of Sony's customer base.

Corrective programme costs

Increasingly the regulatory authorities, on top of the fines imposed, will also require organisations to undertake corrective action which will be monitored and audited by the same authorities. These corrective programmes are designed by the authorities and therefore the scope is often broader and the implementation timescales much shorter than would have been the case under an internally developed programme.

This is also the most common area in which organisations are affected with over 60% of IRM's cyber risk survey respondents highlighting the increased costs of correction action programmes following a breach. This was 24% higher than the next most common, fraud.

These programmes are therefore extremely costly to the organisation with a particular demand on employees through increased overtime or specialist skills brought in on a temporary basis. Indeed the costs of the programmes alone are often many times higher than the original penalty imposed by the regulatory authority.

IT network upgrade costs

Often cyber losses will highlight weaknesses within IT network infrastructure which have been exploited by the cyber threat. For some organisations these weaknesses may have been known and a prior risk assessment determined it was a tolerable risk against the likelihood of the threat. Unfortunately now that this weakness is externally known the likelihood of repetition is certain and therefore the previously costly network enhancements must now take place.

Although these investments are necessary and in most cases good practice to provide adequate assurance against a cyber loss, when the investments are driven by a loss event the time and scale of the spending may fall badly with business planning or at a time of poor business performance. It is therefore the sudden requirement to invest capital in improved IT infrastructure which is the major impact.

Devaluation of intellectual property

The loss of intellectual property can have a devastating impact on an organisation with many not being aware of a theft until a competitor launches a similar or identical product. Indeed a case study described in the supply chain risk chapter (Chapter 7) in this document details similarities between the American F-35 fight jets and the Chinese J-31 fighter jets, with the Chinese designs getting to market first. In the IRM Cyber Risk Survey, almost 20% of organisations suffering a cyber breach were the victims of a loss of intellectual property, the 4th most common business impact of a loss.

It has also been observed that small businesses are particularly vulnerable to this particular loss. Typically small businesses have the weakest cyber security controls, yet they are often disproportionately reliant on their intellectual property. For these organisations a cyber loss may not just be a failed customer tender or being second to market for a new product – it can result in the loss of all income streams and the ultimate closure of the business.

Cyber loss, unfortunately, is one of the most likely events to change senior management perception of the importance of cyber risk management.

Minimising the impact

It is very unlikely and most probably impossible to prevent all cyber losses due to the ever growing frequency and complexity of the criminal efforts to steal data. Indeed in some areas the cost to mitigate the risk may be many times more than the actual loss of that piece of data.

It is however essential to implement controls which can help minimise the potential impact to your organisation. The 2012 UK Government guide on 10 Steps to Cyber Security (see Chapter 16 from CESG for more information) detailed the following control areas that will address 85% of all potential breaches:

- User education and awareness
- Home and mobile working
- Incident management – see Incident Management chapter
- Information risk management regime
- Managing user privileges
- Removal media controls
- Monitoring
- Secure configuration
- Malware protection
- Network security

In addition organisations should ensure that they:

- Implement effective supply chain controls – See supply chain chapter 7
- Develop clear policies for the business use of cloud services – See cloud chapter 8
- Develop clear policies for the use of social media – See social media chapter 10

The required investment associated with many of these controls is explored in more detail in the Investment chapter of this research.

Setting executive team expectations

It is vital that risk professionals within an organisation are able to communicate effectively with the senior leadership on the importance of effective cyber risk management. This is supported by AIG, 2012, which stated that *"It is apparent that data risk management and security must be top of mind for corporate leaders if they are to operate within new regulatory regimes of data privacy around the world".*

Indeed a cyber loss, unfortunately, is one of the most likely events to change senior management perception of the importance of cyber risk management. This too was evidenced in the IRM Cyber Risk Survey with over 76% of organisations which had suffered a breach stating that senior management focus had either significantly or partially changed towards information security.

Ideally the risk function should get the attention of the senior team before a breach occurs. Key to this is being to highlight the potential impact to the organisation of such a breach. This chapter is intended to assist in this process by providing information and case studies on the range of consequences of a breach and show that the business impact is so much more than just a fine.

The risk function should get the attention of the senior team before a breach occurs.

Gaining the executive team support is also a fundamental requirement of getting investment for an information security programme to address cyber risk – See Investment chapter 15.

Tools to assist with risk identification

This section provides risk professionals with some simple tools to assist in the identification of risk impact areas which may affect the organisation in the event of a cyber loss. This information can then be used to aid the development of a business estimate of the financial impact of an event.

Although cyber risk can appear daunting for non-specialist risk managers, the actual identification of risks should follow the same process as you currently utilise. This chapter proposes the following basic techniques, although there should be no reason to divert from your current processes:

- Questionnaires
  - Focus on the key information within the business and the stakeholders who access and use this information.
- Lessons learned review
  - Establish if and how information security breaches within your company or industry have happened and capture the relevant risks for your organisation.
- Stakeholder interviews
  - Conduct one-to-one sessions with key business stakeholders focussing on critical business information and how it could be accessed.
- Workshops
  - Review all the risks identified in the above processes within a workshop of all key stakeholders. This brainstorming approach will draw out new risks which have been missed.

Quantifying the impact

As we saw from the IRM Risk Survey described earlier, many organisations struggle to quantify the impact of a cyber loss after it has happened, so making an assessment of the potential impact can be very difficult for risk professionals. This approach can help to provide an estimate of the possible exposure the business may face from a significant cyber loss – thresholds are only suggestions and should be adapted for your business.

All thresholds should be tested by your IT colleagues to ensure that the appropriate numbers are applied for your own organisation.

This chapter has highlighted the wider business impact which organisations can suffer from cyber losses.

Risk Impact Type	Impact Level		
	Low	*Medium*	*High*
Regulatory Fines	<£50,000	£50,000 to £250,000	>£250,000
Reputational Damage	Difficult to quantify		
Loss of Customers	<£100,000	£100,000 to £1m	>£1m
Loss of Employees	<5% of identified talent	5% – 10% of identified talent	>10% of identified talent
Stock Devaluation	<1%	1% to 5%	>5%
Corrective Programme Cost	<£100,000	£100,000 to £1m	>£1m
IT Network Upgrade Costs	<£100,000	£100,000 to £1m	>£1m
Devaluation of IP	<£100,000	£100,000 to £1m	>£1m

Conclusions and recommendations

This chapter has highlighted the wider business impact which organisations can suffer from cyber losses. Aside from the headline grabbing regulatory fines there are a number of significant areas which are often overlooked by management.

As an effective risk professional it is important for you to be able to communicate the broader impact of a cyber loss to the senior management team and to ensure sufficient focus is given to identifying and mitigating the associated risks. A business wide information security programme is a highly effective way of mitigating a great deal of identified cyber risks and by demonstrating the huge business impact which a cyber loss can cause you can assist the business in developing the cost case for such a programme.

Reading list and websites:

1. Zurich, 2012, *Data Breach Cost – Risks, Costs and Mitigation Strategies for Data Breaches*
2. IRM, May 2013, *Cyber Risk Management Survey*
3. DLA Piper, March 2013, *Data Protection Laws of the World*
4. ICO Website, **http://www.ico.org.uk/**
5. ISO/IEC 27001:2005 – *Information Technology – Security Techniques – Information security Management – Requirements*

6. Bird & Bird, *International Data Protection Enforcement Bulletins* (March 2012, August 2012, October 2012, June 2013)

7. Verizon, *2013, 2013 Data Breach Investigation Report*, **http://www.verizonenterprise.com/DBIR/2013/**

8. Zurich, 2013 *"Meeting the Cyber Risk Challenge"* Harvard Business Review

9. Lawrence A. Gordon, Martin P. Loeb and Lei Zhou, 2011, *"The impact of information security breaches: Has there been a downward shift in costs?"*

10. CESG/BIS/CPNI/Cabinet Office, 2012, *10 Steps to Cyber Security*

11. AIG, 2012 *"Mitigating Cyber Risk"* Financier Worldwide

12. Ponemon Institute, 2010, *2010 Annual Study: US Cost of a Data Breach*

13. Lloyd's, 2013, *An Overview of the Cyber Insurance Market* **http://www.acegroup.com/benelux-en/assets/risk-forum-2013_trevor-maynard_cyber-risk-14-march_v2-0.pdf**

14. Kroll. 2013, *Kroll Special Report – Cyber Security and Investigations*

15. The Actuary website, **http://www.theactuary.com/opinion/2013/02/cyber-reality-time-to-quantify-risk/**

16. Note – 1$ = €0.77 for this research

Questions for the board

1. Which of your company assets are at risk?
2. Which areas of non-insurable risk could affect the business?
3. What would the impact profile be for a typical cyber loss?
4. How effective are your existing controls in managing this impact profile?
5. Which of these areas of impact do you feel is the least well managed?

Appendix 4.1 – Data protection fines by country

Country	Max fine
Argentina	$20,000
Australia	A$1.1m
Austria	€25,000
Belgium	€600,000
Brazil	$1.5m
Bulgaria	€50,000
Canada	$100,000
Chile	$4,250
China	-
Columbia	$670,000
Costa Rica	-
Cyprus	€30,000
Czech Republic	€350,000
Denmark	-
Dubai International Financial Centre	-
Egypt	-
Finland	-
France	€300,000
Germany	-
Gibraltar	£5,000
Greece	€147,000
Honduras	-
Hong Kong	HK$1m
Hungary	€35,000
India	€694,450
Indonesia	5bn Rp
Ireland	€100,000
Italy	€120,000
Japan	JYP 300,000
Lithuania	€570
Luxemburg	-

Country	Max fine
Malaysia	-
Malta	€23,293
Mauritius	Rs. 200,000
Mexico	$1.5m
Monaco	€90,000
Morocco	$72,000
Netherlands	€19,500
New Zealand	-
Norway	€90,000
Pakistan	-
Panama	$150,000
Philippines	-
Poland	€270,000
Portugal	€15,000
Russia	€10,000
Singapore	$1m (Sing)
Slovak Republic	€332,000
South Africa	-
South Korea	KRW 50mn
Spain	€600,000
Sweden	-
Switzerland	CHF 10,000
Taiwan	-
Thailand	-
Trinidad and Tobago	-
Turkey	€5,000
United Arab Emirates	AED 1m
United Kingdom	£500,000
Ukraine	€1,594
United States	-
Uruguay	$60,000

Data from DLA Piper, March 2013, Data Protection Laws of the World – data accurate at time of writing, but no responsibility is taken for the accuracy of the data.

TD XHTML 1.0 Transitional//EN" "http://www
ml" xml:lang="en">
content="no" />
archive" />
cache" />
imageindex,noimageindex" />
ext/css" href="pn_style.css" />
ext/css" href="print.css" media="print" />
png" type="image/png" />
" href="favicon.png" type="image/png" />
plication/rss+xml" href="http://f" title="
ype="text/javascript" src="json2min.js"></
vascript" src="jquery-1.4.4.m

> “Corporate governance is a scheme for ensuring that the executive managers, who have been placed in charge of the company, fulfil their duties.”

Chapter 05: Governance of cyber threat

Chapter 5: Governance of cyber threat

David Canham

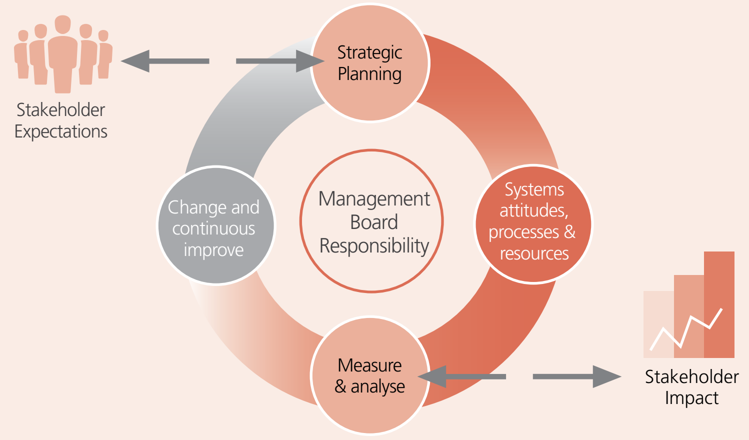
….this chapter will examine whether traditional governance is adequate and question whether organisations give sufficient time and thought at their key committees and boards to the cyber threat…

Governance of the cyber threat is complex and has many layers. Organisations are increasingly exposed to the outside world through digital offerings and access to the internet both for business purposes and personally by staff. Organisations are increasingly interlinked and cooperation between public, private and the state is paramount in understanding the range of threats and sharing "best practice". With such a wide ranging and multi-faceted threat landscape this chapter will examine whether traditional governance is adequate and question whether organisations give sufficient time and thought at their key committees and boards to the cyber threat that in some cases they cannot clearly see or articulate.

This chapter will examine the current capacity and mandate of oversight structures within organisations. Further, it will examine the pace of technological change when considered alongside the pace of regulatory change and consider if the existing regulatory frameworks enhance or constrain organisations attempting to govern the cyber landscape.

This chapter will also consider the importance of accountability in relation to managing the cyber threat and how that influences the development of international standards and setting security expectations to provide an effective framework for managing the cyber-risk landscape.

When thinking about cyber governance it is clear that the challenges are many and varied with an increasingly faceless threat, immediacy and speed of attack as well as complex motivations. Organisations need to be clear on their responsibilities, preventive measures and their ability to react to incidents. Indeed, with intelligence agencies providing advice and governmental concerns over protection of the critical national infrastructure, there is a degree of the cyber threat that is outside of the organisation's direct control. The next sections will examine the traditional approach to Governance and will then go on to explore what differences may need to be recognised or built into governance frameworks in order to deal with the cyber challenges.


Stakeholder Expectations
Strategic Planning
Management Board Responsibility
Systems attitudes, processes & resources
Change and continuous improve
Measure & analyse
Stakeholder Impact

> Traditional governance measures are challenged by a cyber environment.

Traditional governance models

Before we start on the challenges that cyber risk presents to governance models, let us briefly discuss what we mean when we talk about governance. There are a number of models available to define governance. However, we have adapted the model taken from the Institute of Directors' "Director's Handbook" as shown opposite. This shows that it is the management board's responsibility to direct and control the company so that the right systems, attitudes, processes and resources are in place to implement the strategy that will meet the stakeholder expectations. These are then measured and analysed over time to identify areas for continuous improvement and change that will sustain the longevity of the organisation, thereby meeting the stakeholder expectations. Or, as the Corporate Governance Committee of Japan states,

"Corporate governance is a scheme for ensuring that the executive managers, who have been placed in charge of the company, fulfil their duties."

The UK Corporate Governance Code (formerly the Combined Code) sets out standards of good practice in relation to board leadership and effectiveness, remuneration, accountability and relations with shareholders.

The landscape challenge to governance

There is much written about governance codes and the way in which organisations respect or abuse their own governance systems and controls. Notable examples of poor practice include Enron, Polly Peck and Hollinger International. However, when talking about cyber governance a different landscape applies. The traditional internal bad practice, financial irregularity or director fraud is not the key risk focus. A new breed of threat exists that is characterised by being faceless, borderless and can be perpetrated inside or outside of the organisation by factions, organisations or territories unknown. It can infiltrate organisations and remain dormant for some time before becoming active and detectable but at that point, it is almost too late. The damage could already be done.

Cyberspace is a concept that has grown at a phenomenal rate and organisations have not necessarily been able to keep pace with it or gain a full understanding of the context to be able to respond to the opportunities and challenges it brings. Traditional governance measures are challenged by a cyber environment that presents a dynamic risk to the fitness of such traditional governance measures. These measures could currently involve:

- reactive committee structures,
- static policies,
- partially educated staff and
- reasonably static risk management based on quarterly reporting cycles

So, in defining cyber governance we need to understand what cyberspace is. The Democratic Governance Challenges of Cyber Security (DCAF) defines cyberspace as "the independent network of information technology infrastructures. It includes the internet, telecommunication networks, computer systems and embedded processors and controllers in various industries". In reality, cyberspace touches us all in our daily lives, be this through our work or social activities, and the challenge for organisations is to govern the usage of this freely available, unregulated environment to protect, enhance or build on a reputation.

Whether it is at board level or on the shop floor, the pervasive nature of the digital presence has the potential to have a real time impact both personally and at corporate level. Understanding an organisation's digital presence is paramount if the risk is to be effectively assessed and managed. Further, the explosion in the use of the internet, social media (see Social Media chapter) as well as the increase in digital marketing and sales channels, fundamentally changes the operational landscape we both live and work in. As a result, the challenge to organisations ranging from one man enterprises, SME's up to large global corporations is fundamentally changed.

Organisations now find themselves operating in a cyber-landscape where knowledge, reputation and customer views can be shared or lost in an instant. Social media has led to a situation where comment can be shared instantly and the governance of the response is now equally as important as to the preventative measures. Organisations are also increasingly concerned about a faceless threat from parties unknown that can disrupt on-going operations via the tap of a keyboard or click of a mouse.

To deal with these challenges, governance dictates that certain things need to be in place such as:

- clear policies and processes
- defined roles and responsibilities
- defined accountabilities, and
- established committee structures

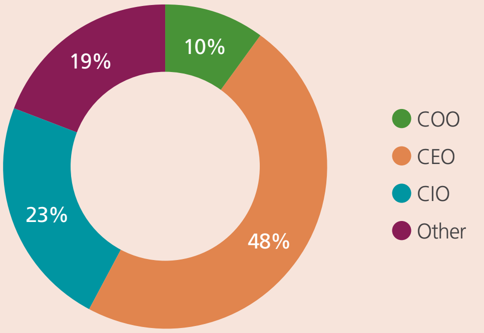
In research commissioned by the IRM RISE SIG it was found that organisations do recognise this. However, the effectiveness of these measures is questionable. Some examples from our survey are outlined below:

- Of 144 respondents who have an Information Security Programme, 63% had a training and awareness regime in place.
- Of 170 respondents to the question "Do you have an Information Security Programme in place with completion rates monitored?', only 55% stated yes, with a further 20% stating partial monitoring.
- Of 144 respondents who have an Information Security Programme, only 33% answered 'yes, always' to reviewing the effectiveness of supply chain controls.

Further, in terms of the establishment of clear governance roles and responsibilities the survey found that 48% of the 172 respondents saw accountability resting with the CEO, as illustrated opposite.

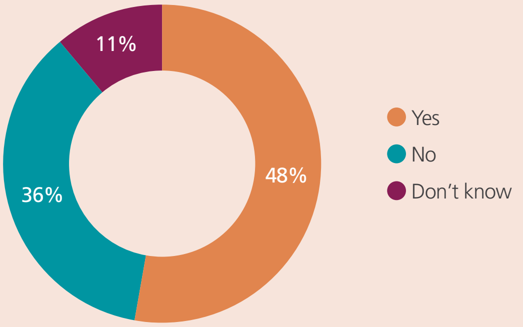
> Organisations now find themselves operating in a cyber-landscape where knowledge, reputation and customer views can be shared or lost in an instant.

Where responsibility for information security resides



In terms of committee oversight, the IRM survey found that of the 171 respondents, only half had a designated committee to oversee information security risk despite the plethora of media stories on the subject and the increasing levels of fines being levied around the globe on organisations that have a breach.

Do you have a specific committee that meets to discuss information security and provide oversight of information security risks?



When assessing the cyber-landscape it is useful to consider the cyber threat categories.

The responses we received suggest that there is still a way to go in achieving effective governance of the information security regime in organisations. Respondents were unclear on where accountability lies in the boardroom and the education and oversight felt weak with limited views of the information security risk by committees. Additionally, our survey results revealed that there was poor tracking of information security education and awareness programmes. It was not clear, however, if this was an issue with the risk manager awareness on the subject, or symptomatic of the fact that information security and the "cyber" threat is seen as the domain of the techie. Nevertheless, the reality is that it is an organisational wide issue where culture plays as an important role as control and technology does.

When assessing the cyber-landscape it is useful to consider the cyber threat categories. The following table, taken from the DCAF paper, gives a useful overview of the types of attack seen and also reinforces the point that, unlike traditional views of cyber threat, not all those wishing to exploit an organisation are motivated by theft.

Governance: traditional approaches

When considering governance there are a multitude of models that can be adopted but for the purposes of this paper four cornerstones are considered. These are:

- **Delegated authorities framework – "what people can do"**
  - Defines specific limits of authority within which employees may approve financial and non-financial activities on behalf of the company
  - Links into individual's Roles and Responsibilities
- **Committees – "how oversight is provided"**
  - Responsible for management of the business and providing oversight and challenge to support the achievement of key objectives
- **Organisational policies/standards – "high level organisational principles"**
  - Defines processes and responsibilities for the management of risk
- **Risk management – "informed decision making"**
  - Facilitates the setting of appetite for risk
  - Process for identification, assessment and reporting of key risks
  - Agreement of actions to mitigate risks that are outside risk appetite

Table 5.1. Categories of cyber threats

Category	Sub Category	Example
Integrity Cyber-attacks may use hacking techniques to modify, destroy or otherwise compromise the integrity of data.	Propaganda/ disinformation	Modification or manipulation of data or introduction of contradictory data to influence a political or business outcome or destabilise a foreign regime.
	Intimidation	Attacks on websites to coerce their owners (both public and private) into removing or modifying content, or pursuing some other course.
	Destruction	Permanent destruction of data to hurt competitors or attack foreign governments. This may, for example, form a part of wider conflict.
Availability Denial of service attacks by botnets, for example, may be used to prevent users from accessing data that would otherwise be available to them.	External information	Denial of service, etc. attacks on government or private services available to the public, for example, media outlets, government information sites, etc.
	Internal information	Attacks on private or governmental intranets, for example, emergency services networks, energy and transport control infrastructure, e-banking sites, company email, command and control systems
Confidentiality Cyber-attacks may target various types of confidential information, often for criminal gain.	Espionage	Firms seeking information on their competitors; states involved in spying activities (against both foreign states and individuals).
	Personal data theft	Phishing attacks (or similar) aimed at tricking users into revealing personal data, such as bank account numbers; viruses that record and upload such data from a user's machine.
	Identity theft	Trojan horses, and so forth, used to steal identity information that is then used in the commission of crimes.
	Data mining	Open source techniques employed to discover, for example, personal information from publicly available data.
	Fraud	Often delivered via spam email, fraud includes the popular Nigerian "419" or advanced fee fraud, as well as attempts to convince recipients to buy a range of fraudulent goods or services.

Attitudes, values and behaviours that flow through the culture of the organisation a re crucial to the effectiveness of governance and the ability to meet the modern cyber threats.

It is also important to note that the attitudes, values and behaviours that flow through the culture of the organisation are crucial to the effectiveness of governance and the ability to meet the modern cyber threats. Bureaucratic organisations with tight traditional governance structures may find that governance is slow moving and committee based, organisations that are younger with more free flowing attitudes are likely to be able to move quickly to address cyber challenges. Further, the different value systems in organisations will potentially impact the effectiveness of governance and potentially the attitude to cyber risk. For instance the organisation targeted on aggressive growth is potentially less likely to be willing to invest in underlying security controls than one that's more prudent and balanced in their strategic aims on protecting the existing operation.

Regardless of the value system of the organisation it is important that throughout the governance structures employed, lessons are learnt and messages permeate the organisation to allow the response to the cyber threats faced evolve appropriately and intelligence is shared. So taken each element in turn in terms of practical advice and assessment the following sections will give some insight.

Delegated Authorities

The delegated authorities to commit the organisation to spend, enter a partnership, outsource or external relationships, etc. will vary depending on the size and shape of the organisation and the nature of operations. However, from a practical view point there are some key points for consideration which we discuss further below and these are:

- Does the delegated authority take into account the "cyber" environment?
- What is the accountability for prevention and response?
- What is the Governance for delegated authority in the extended enterprise?

Does the delegated authority take into account the "cyber" environment?

For instance, is there a need for a more dynamic sign-off process? Traditionally, larger organisations have strict protocols from the shop floor level to board level to sign-off and commit the enterprise to a course of action. In some cases this involves a number of sign-off loops and paper production. In a world where cyber opportunities and threats evolve in real time, traditional authority routes may not be fit for purpose and may need to be more agile. Decisions such as who holds the authority to use the corporate twitter account or who has the authority to invoke emergency crisis measures in the event of a cyber-attack need to be clear. Roles and responsibilities need to be defined because from a practical view point, in this particularly media centric world of instantaneous global communications, inaction due to lack of clear authorities can be equally damaging as the event itself.

What is the accountability for prevention and response?

For those organisations operating in the real-time cyber-world, which is probably the vast majority of businesses, clear accountability is paramount. When an incident occurs the leadership and accountability has to be clear and has

> Values and behaviours that flow through the culture of the organisation are crucial to the effectiveness of governance and the ability to meet the cyber threats.

to be known upfront as we discuss in the Incident Management chapter later in this research. Also, when an opportunity can be seen in the market place, organisations need to be clear on who owns the response and be clear on the roles of, for example, marketing and communications or security. Practically, from what is witnessed through the IRM RISE SIG perspective, organisations struggle with who leads on cyber issues such as social media, cyber response, strategy etc.

What is the governance for delegated authority in the extended enterprise?
Increasingly, organisations are networks of interconnected organisations ranging from the small enterprise to the multinational with a network of suppliers, distributors, regulators and customers all of whom have an interest in the organisation. Some of these groups will have delegation and authority to act on behalf of the extended enterprise. Governance of these delegations is equally as important for the prime organisation to understand and exercise.

Committees

Traditional committee structures provided oversight on a periodic basis with usually lag Management Information[7] making decisions and documenting these on an informed risk basis. However, with so much in an organisational agenda the management and oversight of information security risk is often the preserve of committees in the CIO / CISO directorate structure or the technology department.

If information security is truly the responsibility of the CEO and a business problem, the challenge is to move oversight away from solely technical governance committees into the strategy and business management processes. As mentioned earlier in the RISE survey only 53% of respondents had a specialist information security committee. So in considering this from a practical viewpoint, the following points should be considered:

- The structure, capability and seniority of committees
- The use of management information to inform debate

Structure, capability and seniority

Does the committee structure your organisation adopts consider the authority required to drive the appropriate culture and make informed investment choices to respond to the cyber threat? Further, does the committee understand the nature of the risk? The results of our survey highlighted that most organisations do not have in-house specialists with 49% relying instead on external advice. To make matters worse, our research found that the translation of technical cyber security risks into a language that the boards and senior leaders could understand was a significant challenge. This is particularly important where budgetary decisions are required. If the importance is not recognised, investment and momentum behind mitigating and addressing cyber risks is lost over the growth imperatives of the organisation.

[7] Lag MI looks at retrospective indicators to inform movement in risks and supporting decision making

Designing and using lead indicators requires a collaborative approach across the business.

Use of management information to inform debate

Management Information (MI) is used to drive business decisions. MI can take the form of lag or lead indicators[8]. It is always a challenge in organisations of all sizes to find adequate lead indicators. Most governance committees will look at lag measures and base oversight decisions on these. Consequently, traditional lag measures are reactive in nature and in terms of the emerging and fast-paced cyber threat, may not be sufficient to inform the cyber risk management debate. External case studies are useful, TK Maxx and Sony for instance, but practically applying lead indicators in your organisation to spot trends and potential incidents is difficult. When considering governance committees and the MI they will need, particularly if they look at vulnerabilities or incidents, a more real time approach has to be adopted. Designing and using lead indicators requires a collaborative approach across the business. Nevertheless, spending time reviewing and creating clear and concise MI is usually time well spent.

TK Maxx – Case Study

Hackers stole information from at least 45.7 million payment cards used by customers of US retailer TJX. The firm said it did not know the full extent of the theft and its effect on customers. TJX stated the security breach may also have involved TK Maxx customers in the UK and Ireland but felt that at least three-quarters of the affected cards had expired or data had been masked. The data was accessed on TJX's systems in Watford UK and Massachusetts USA over a 16-month period from July 2005 and covered transactions made by credit and debit card dating as far back as December 2002.

Taken from BBC Website March 2007

Organisational Polices / Standards

Key to the management of risks and the governance framework of an organisation are its policies and standards. These should set out minimum controls, culture and approach to how an organisation should behave. In information security risk these are equally important and crucial in managing the control environment. There are a number of practical considerations including:

- Policies and standards tailored to the audience
- Education and awareness is a key component
- Considering the extended enterprise

[8] After event indicators used to adjust or measure the assessment of a risk

Policies & standards tailored to the audience

Ensuring policies and standards are tailored to fit the intended audience is key. For example, most organisations will have technical standards that are designed for the IT community to mandate activities such as secure email, secure applications development etc. These will be written in a clear way and set out a technical standard of control, potentially in line with International Standards. Other policies, such as use of communication systems, social media etc. will be aimed more at all the staff in an organisation and as such, they need to take into account the culture of the organisation and the knowledge and competencies of the audience. Differences in these groups must be understood and policies and standards written that are fit for purpose.

Education and awareness are key components

Organisations can have the best policies and standards in place but without an appropriate education and continuous awareness programme they become shelf-ware. Many organisations will rely on annual computer based training (CBT) but with an ever-changing threat landscape it is recommended that there is an increased level of awareness. To support CBT, organisations should consider the practical application of more regular targeted awareness bulletins using multiple communication channels. One example is to post bulletins about a breach or incident that has appeared in the media and extract one or two key messages that all staff should note as applying to the organisation. Quick and dirty messages that react to other people's misfortunes but help to keep the message alive within the business are effective.

Considering the extended enterprise

As an organisation sets its own policies and standards it also needs to consider the extended enterprise and how it will gain assurance that the same principles are being applied. There are a number of ways to do this, including:

- placing stipulations in contracts to act in accordance with the parent policies/standards
- carrying out a standard audit through an accredited supplier aligned to an international standard
- carrying out your own audit programme.

However an organisations looks to control this, the underlying principle should be that the parent organisation needs to protect its reputation and its data across the extended enterprise.

> “Risk management is a key process that informs the other elements of the governance framework and provides the insight into the health of that framework.”

Risk management

Risk management is a key process that informs the other elements of the governance framework and provides the insight into the health of that framework. Through understanding the risk profile, delegated authorities can be reviewed and the polices and standards can be amended. In addition the external insight that risk management brings can help to bridge the translation issue between technical staff and business leaders providing they all understand the key components involved. In terms of practical considerations, these include:

- The role of risk appetite, tolerance and categorisation
- Key risk indicators
- Risk identification and assessment
- External intelligence

The role of risk appetite, tolerance and categorisation

Risk appetite, tolerance and categorisation are key factors for any organisation to understand and are a catalyst in supporting the investment case for "cyber" (See investment chapter). The risk manager, when considering cyber risk, needs to be able to articulate in simple business terms the nature and scale of the risk faced by the organisation and the tolerance/appetite a business should consider. Senior management can then make a reasoned decision through governance committees or delegated authorities about the investment required to achieve this appetite / tolerance position. The practical challenge for the risk manager is provoking this debate in a crowded organisational agenda where pressures to grow or deliver service compete with those of security.

RISK APPETITE – "Do you really mean that?"

"We have no appetite for a data loss or security breach" could be translated into "I am going to throw as much money as it takes to build my cyber fortress". In other words, the IT department and the information governance efforts have a blank cheque. Do we really mean that or are we going to accept that a breach/incident is inevitable and we really want to prevent the preventable?

Key risk indicators

In previous sections the chapter has considered Management Information. MI fulfils another core role in the risk process through the use of key risk indicators. These indicators help the risk professional and the business to track the movement and attempt to predict changes in the nature of risk, providing an insight into the health of the mitigating controls and helping inform governance mechanisms on decisions. Cyber risk is no different; the challenge is to find indicators within the organisation to give this intelligence. In terms of indicators the risk manager needs to consider three core types:

The practical challenge for the risk manager is provoking this debate in a crowded organisational agenda.

- Lead – forward looking indicators used to predict and shape changes in a risk's profile
- Lag – after event indicators used to adjust or measure the assessment of a risk
- Countermeasure – measurement of current control action effectiveness in terms of an assessed risk

In an ideal world a mixture of the three types would be ideal but it is not always possible to identify these. External benchmarking, your own organisation's management reporting or risk event analysis is a good place to start to build these metrics.

Risk identification and assessment

Identification and assessment is the bedrock of risk assessment. The risk manager will take the standards and polices, together with business strategies and objectives, to realise a complete assessment of the risk environment including the security landscape. This view of the risk is usually measured by probability and the impact and subsequently played back to key stakeholders. This supports the committee oversight of cyber risk and the relative importance of each risk to the other and informs the debate from the shop floor to the boardroom on what the remediation priorities should be.

External intelligence

External intelligence is another area where the risk management process can assist the organisation in managing cyber risk. Through a network of contacts, external horizon scanning and the use of trusted public domain surveys and risk reports, intelligence from outside the organisation can be brought to the decision makers. However, despite a push by the British Government to be open about breaches to improve external intelligence and knowledge sharing, there remains a reluctance to share information on breaches. Our survey found that while 61 out of 232 respondents indicated that data breaches had impacted their business, only a small handful were then prepared to share any detail.

We have considered a simplified governance model and given some practical thoughts some of the issues facing organisations. We will now consider how the challenges may be different in a cyberspace environment.

Cyber governance: is it different?

The previous section considered the cornerstones of traditional governance, in this section the chapter considers different practical challenges cyberspace brings. The Information Security Forum (ISF) outlines principles and objectives for security governance, namely

Principle – A framework for information security governance should be established and commitment demonstrated by the organisation's governing body

Objective – To ensure that the organisation's overall approach to information security supports high standards of governance

Source – Information Security Forum, the Standard of Good Practice Governance Page 14.

The threats posed by cyberspace means that organisations must develop clear policies and standards.

Commitment on the corporate agenda

Advocacy is crucial to any topic. Risks or issues gaining airtime and staying on the organisational agenda is no different. As the ISF suggests, ensuring clear roles and responsibility in relation to cyber risk in the boardroom is key, not only to set direction and policy, but to secure any necessary funding. Organisations, by their nature will not always see information security as the top of their investment list. At worse they may see it as an overhead or expense to achieving the strategic aims. Executive sponsor nomination and clear accountability is essential if organisations are to ensure commitment to security investment, whether that is financial or time investment. It is also important for good governance.

Further it is vital that the issue of cyber and information security is not buried in IT or CISO governance structures as the impacts and controls reach much wider as we will demonstrate throughout this guidance document. Technical protection is important, but in an increasingly digital world the social engineering and cultural challenges are equally, if not more important as people need to understand why they are doing things and what to watch out for. As the IoD governance model alludes to, tone from the top is vital to set the right attitudes and behaviours and business ownership on the corporate agenda sends a clear message that the executive level take the subject seriously and everyone else should do so too. All staff are responsible for security.

Corporate or personal education or both

The threats posed by cyberspace means that organisations must develop clear policies and standards. However with organisations using cyber space to market their wares, increase sales or even profile prospective clients or recruits, the applicability of these policies to an individual’s personal life and corporate life becomes blurred. Take for instance the CEO using their own personal Twitter account to talk about company business. What happens when they move on? Or the claims handler befriended over LinkedIn by a broker or IFA for preferential treatment, or in extreme cases the staff member threatened or manipulated over social media to carry out malicious activity? Organisations have a practical duty to raise awareness of organisational policy but they may also need to consider the typical usage scenarios and consider education of staff in a way that handles those blurred boundaries.

Compliance, regulation and the law

Many organisations are operating within a regulatory or compliance regime. In addition, there are local and international legal stipulations of which organisations need to be aware. However simply complying with the basic stipulations is not necessarily demonstrating compliance. Under the “comply or explain” principle of corporate governance, as stipulated by the UK Corporate Governance Code, with similar requirements in many other territories, those organisations putting growth over protecting the security interests and doing the “minimum” to get by, run an

It is vital that information security governance incorporates cyberspace across the extended enterprise, is sponsored at the executive level and has sufficient space on the corporate agenda and key governance forums.

increased reputational and regulatory risk. International law is complex and includes directives such as the EU Data Protection Regulation (which is due in the next year or two), so organisations need to ensure their governance structures demonstrate an awareness and appreciation of the legal and regulatory environment within which they operate. Further, as regulation struggles to keep pace with the speed and complexity of the threat, organisations have very real financial and technical challenges to be able to meet compliance requirements particularly if they have large legacy infrastructures.

Recent UK Financial Conduct Authority rulings have also highlighted there is little appetite for financial institutions using resource and cost pressure as an excuse for non-compliance or error. For example, in its findings in relation to inappropriate reporting of third party transactions at RBS, the FCA stated that "*… given the considerable resources available to RBS, it should have been able to overcome these challenges and ensure adequate systems and controls were in place"*

Accessed via http://fca.org.uk/rbs-fined.

Pace of threat vector innovation and organisational governance

The threats and attacks from a cyberspace are increasingly complicated and their innovative and rapid deployments are challenging traditional organisational governance models. Furthermore, some threats can often be "sleeping" or "silent"; lying dormant for 6 months or more before they are activated. In the UK, the first an organisation may know of a threat could be when intelligence agencies such as Government Communications Headquarters (GCHQ) informs them of a cyber-intrusion affecting the national critical infrastructure. Consequently, there is a need for organisations to have robust governance processes in place that support quick and effective decision making based on clear roles and responsibilities (as we discuss further in the Incident Management chapter). In a world where a cyber-attack can get worse by the minute, governance has to be swift and reaction plans well-defined in bid to contain and limit any organisational damage.

Conclusions and recommendations

There are some basic steps an organisation of any size can take to put in place effective governance for cyberspace. To begin with, the current data / information security governance framework can be reviewed and organisations can run stress scenarios to consider how they would react and respond to a real time incident.

In addition there is guidance for organisations aimed at both boards and at the more technical level, such as the UK Government's 10 steps to Cyber Security:

www.bis.gov.uk/assets/biscore/business-sectors/docs/0-9/12-1120-10-steps-to-cyber-security-executive) (also summarised in Chapter 16 of this document) and

Cyber Risk Management – A Board Responsibility: **www.gov.uk/government/uploads/system/uploads/attachment_data/file/34593/12-1119-cyber-risk-management-board-responsibility.pdf).**

It is vital that information security governance incorporates cyberspace across the extended enterprise, is sponsored at the executive level and has sufficient space on the corporate agenda and key governance forums. The Information Security Forum recommends the CISO has a direct line to the governing body of the organisation or via a senior member of an independent risk function to enable this to happen. It is strongly recommend that this is a minimum and that the cyber and information security is embedded, understood and clearly articulated throughout the organisation using risk management principles to provide informed direction and effective governance with increasing agility.

Questions for the board

1. Is "cyber" on the board agenda?
2. Is your governance structure dynamic enough to react to "real time" threats?
3. Do you have dynamic risk assessment processes to assess, manage and react to cyber threats?
4. Are the lines of delegation and response clear in your organisation to allow speed of decision making in reacting to a cyber incident?
5. Are your security policies, processes and procedures clear and understood throughout your organisation?
6. How comprehensive is your education and awareness programmes in security and do they consider personal and professional accountability?
7. Does your enterprise work across multiple territories with different legislative and regulatory regimes?
8. Do you have sufficient Management Information and External Intelligence to monitor your threat exposure?

Reading list and websites

17. *Information Security Forum, The Standard of Good Practice Governance* – June 2013

18. *CESG/BIS/CPNI/Cabinet Office 10 steps to Cyber Security accessed* via **http://www.bis.gov.uk/assets/biscore/business-sectors/docs/0-9/12-1120-10-steps-to-cyber-security-executive)**

19. *BIS, Cyber Risk Management – A Board Level Responsibility*, July2013 accessed via **https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34593/12-1119-cyber-risk-management-board-responsibility.pdf**

20. ISACA – *The Computer Forensics and Cybersecurity Governance Model* **http://www.isaca.org/Journal/Past-Issues/2003/Volume-2/Documents/jpdf032-ComputerForensicsandCybersecurity.pdf**

21. *DCAF – Democratic Governance Challenges of Cyber Security* – 2009 **- http://www.dcaf.ch/Publications/Democratic-Governance-Challenges-of-Cyber-Security**

22. *FCA – RBS Ruling* – July 2013 accessed via **http://fca.org.uk/rbs-fined**

23. *BBC – Hackers Target TK Maxx Customers – March 2007 accessed* via **http://news.bbc.co.uk/1/hi/business/6508983.stm**

> “This chapter is intended to demystify some of the opportunities cyber and the digital age offers. And it suggests how enterprises can better exploit these in a secure manner.”

Chapter 06: Managing Business Opportunities and Information Risks

Chapter 6: Managing Business Opportunities and Information Risks

BAE Systems Applied Intelligence

This chapter is intended to support executives in enterprises with responsibility for risk.

Abstract

So what does 'cyber' or 'the digital age' mean to you? It's likely to depend on who you are, where you sit in the enterprise and what you are responsible for. For boards and senior executives, it is often seen from two polarised positions; from the incredible range of new opportunities they offer to improve efficiency and open new channels to customers or as a recognised threat that is not properly understood. This thinking is exacerbated by the frantic pace of technological innovation and its adoption, often by the business rather than IT, which is making "just keeping up" difficult.

This paper is intended to demystify some of the opportunities cyber and the digital age offers. And it suggests how enterprises can better exploit these in a secure manner. The paper illustrates the challenge with different scenarios that BAE Systems Applied Intelligence have been involved in with different customers. These illustrate how cyber security can be exploited as an enabler rather than a blocker to the successful pursuit of business opportunities.

Introduction

Research indicates that organisations identify two key functions at the core of their ability to achieve business objectives and pursue strategy. These are:

1. Opportunity management: the ability to identify, pursue and win business opportunities that will provide revenue and grow the business and innovative means to deliver better service to customers and citizens; and
2. Risk management: the need to wholly understand and manage the full spectrum of risk that is faced by an organisation.

Further, the effective management of risks and opportunities is increasingly seen as:

- A vital competitive differentiator, helping organisations achieve success and resilience during difficult economic times; and
- A key factor in demonstrating distinctive organisational attributes to the market such as agility, integrity and trust.

This chapter is intended to support executives in enterprises with responsibility for risk. It will highlight effective tools that can help to ensure an effective balance between opportunity and risk. It also raises pertinent questions that risk officers can legitimately raise to the board in the event they feel there is imbalance in their enterprise.

At the heart of this paper is an exploration of the interaction between opportunity and risk management and the potentially damaging effects of a lack of appropriate balance in this relationship. Finally we present a set of five scenarios of emerging cyber enabled opportunities that challenge existing models and question how these opportunities can be exploited securely.

These scenarios are based on our experience of helping organisations understand the importance of their critical information assets and the level of risk posed to those information assets; and in implementing an appropriate and commensurate set of controls that protects these information assets in line with their risk appetite and in supporting the business in the pursuit of its strategy.

Technological innovation continues to radically impact and change the way society and business interacts and operates. Indeed, in the Harvey Nash CIO Survey 2013 71 per cent of respondents believed that their organisation had to embrace new technology or risk losing market share[9]. It is only right that this book contains a chapter on how risk officers can support their organisations benefit from the opportunities these innovations present, but in a secure manner.

Balancing opportunity and risk management

We now all live and work in a 'connected' world. Our business and personal domains are blurring and this has helped to create a bewildering growth in the potential opportunities available to organisations. But it has also significantly increased the risks they face. Reduced 'barriers to entry' have swelled the number of threat actors seeking to exploit this connected world to their own benefit, be it fraudulent activity for financial gain, cyber espionage or the promotion of activist movements.

Within the information security domain, both risk and opportunity management as well as the interaction between them is gaining increasing focus. For example Chief Information Officers have responsibility for safeguarding their organisations data with appropriate cost effective controls, whilst also enabling business activities to fully realise the opportunities this information offers.

Most mature organisations will have processes in place to manage risks and to identify and track opportunities. But how many ensure that the two processes are aligned and that appropriate engagement between risk and opportunity management exists?

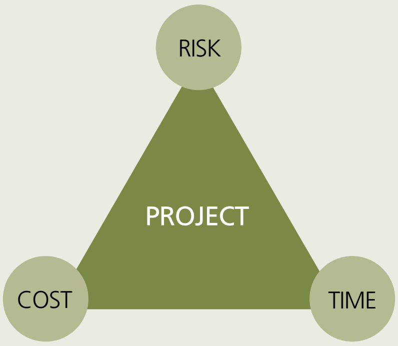
Too little alignment between risk and opportunity management can impact on business performance if each function pulls the organisation in an opposite direction. Too much focus on business opportunity can expose the organisation to levels of risk far in excess of stated tolerances. Too much focus on downside risk on the other hand can create stagnation.

The ideal situation is where cyber risks are considered properly and as an integral part of the opportunity management process. The components of this balance between opportunity and risk management are illustrated in Figure 6.1 which considers:

- Time: what is the urgency of exploiting the opportunity and if so what is the risk appetite in this situation? If timescales are short, does this increase the security risk to the organisation?

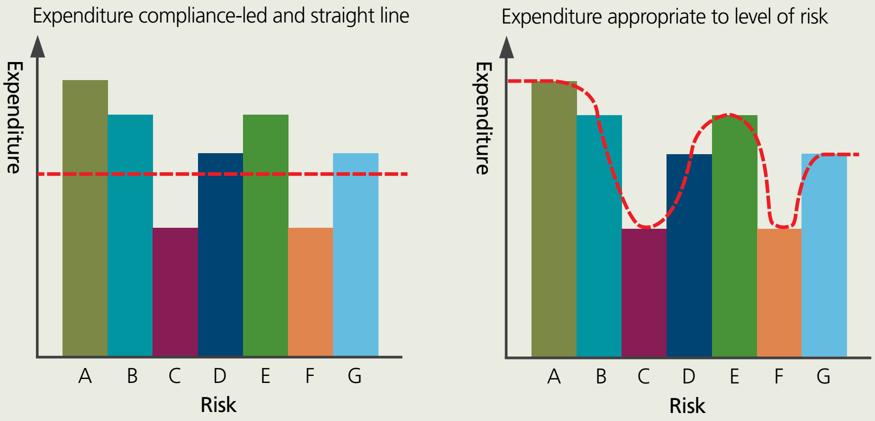
[9] Harvey Nash CIO Survey 2013

Figure 6.1: The components of opportunity and risk management



- Cost: what is the cost of implementing controls for a certain security risk? Does this cost still make the opportunity financially viable? Is this cost considered acceptable in order to meet business strategy?
- Risk: what is the risk that the information to be used as part of an opportunity can be compromised? Can the integrity of this information be ensured as part of the opportunity?

Figure 6.2: Expenditure versus risk



> A common issue we see is that organisations base their risk management plan on a compliance-driven approach.

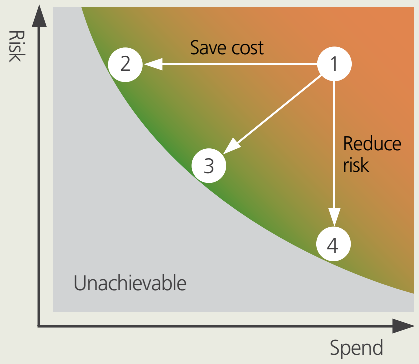
It is also worth noting that once the opportunity has become 'business as usual', it is important that risk management remains involved to ensure that the opportunity remains viable and that the security risk remains within the corporate risk appetite.

A common issue we see is that organisations base their risk management plan on a compliance-driven approach. This can be driven by operating in a regulated industry that blinkers risk management to other models, or which focuses too heavily on impact over likelihood. Adopting this approach can impact opportunity management by creating areas of over-control while also exposing the organisation to additional exposure by under-controlling other areas. This is illustrated in the two graphs below left.

The left-hand chart shows restrictions of a compliance-led approach with the straight line expenditure response, regardless of the risk. Areas above the red line are indicative of being over-managed and correspondingly those below are undermanaged. It is important to use an approach that ensures controls are appropriate and commensurate to the level of risk, as illustrated in the right-hand diagram. This approach can also ensure the response is supportive of the organisations strategy and objectives and allows for a more flexible risk tolerant approach to larger opportunities over smaller ones.

A second key issue we commonly see is that enterprises are not extracting the greatest value from existing spend. Risk officers increasingly demand not only a better return on their investment but also to ensure that risk management decisions are aligned with corporate strategy. This is illustrated in the diagram below.

Figure 6.3: Risk vs. Spend options



> Risk officers increasingly need to ensure both a better return on investment and that risk management decisions are aligned with corporate strategy.

> Most mature organisations will have processes in place to manage risks and to identify and track opportunities.

This lack of balance was identified in one organisation where there was an expectation that any improvement of security controls would be at the direct expense of their ability to pursue opportunities. Through a risk assessment it was determined that existing controls could be better exploited at no extra cost and with positive impact in being able to pursue the opportunities – but now in a secure manner.

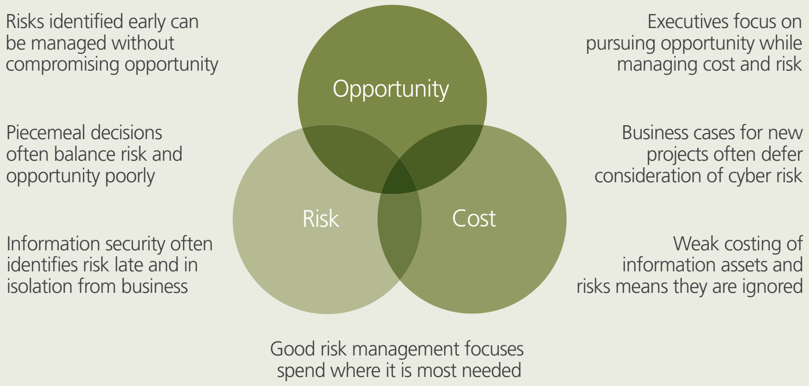
So far we have addressed how risk officers can look to derive the greatest value and benefit from their risk management controls. This goes some way to helping ensure risk management is cognisant of, aligned with and supports the enterprise strategy. But how can risk managers ensure the wider enterprise is mindful of risk as it identifies and pursues opportunities?

A key foundation is ensuring that an appropriate risk governance structure is in place that recognises the relationships and inter-dependencies between risk and opportunity and the associated costs of each. This is illustrated in the diagram below with the impacts to the enterprise, both positive and negative explained where the weighting is wrong.

Successful recognition of these inter-dependencies and the adoption of a framework that ensures the enterprise can be effective and efficiently balance risk and opportunity will help deliver significant benefits. These include:

- A risk management function that is aligned with and supportive of the wider business objectives and strategy. Organisations that fail to pursue opportunities because they are unable to mitigate risks will struggle to grow or be profitable in the current economic climate.

Figure 6.4: Interaction between risk, cost and opportunity


Risks identified early can be managed without compromising opportunity
Piecemeal decisions often balance risk and opportunity poorly
Information security often identifies risk late and in isolation from business
Opportunity
Risk
Cost
Executives focus on pursuing opportunity while managing cost and risk
Business cases for new projects often defer consideration of cyber risk
Weak costing of information assets and risks means they are ignored
Good risk management focuses spend where it is most needed

A key foundation is ensuring that an appropriate risk governance structure is in place that recognises the relationships and inter-dependencies between risk and opportunity and the associated costs of each.

- An ability to react in an agile and confident manner to new opportunities that arise as a result of technological innovation and new business models that will arise as a result. The enterprise will be able to thrive in uncertain and increasingly competitive times because it has the appropriate flexible risk mitigation in place commensurate to the level of risks and opportunities faced; and
- A more resilient enterprise that is better prepared to react in the event of a cyber incident. Demonstrating robust risk management processes protects reputation and allows organisations to build confidence and trust in relationships with partners, customers, suppliers and in new markets.

In the following section we outline four scenarios illustrating some of the risks and opportunities associated with emerging technologies being adopted in the enterprise.

Scenario 1: Mobile devices (Bring Your Own Device & Bring Your Own Technology)

On the face of it there should be a clear cut case for enhancing operational productivity by introducing personal mobile devices into the enterprise. Models for how this might work already exist – for example those in place for company cars – that would only need some adaption for mobile devices.

In reality managing the opportunities and risks of personal mobile devices is far more complex. Typically it is rare that the business case for staff to bring their own mobile devices or technology into the enterprise has been fully considered, let alone documented. Correspondingly there are usually no performance or risk indicators assigned to measure whether implementation delivers the predicted benefits of increased efficiency and productivity.

Delta airlines recently announced they would be supplying tablets to all of their pilots. They will replace paper copies of flight manuals and maps with an estimated saving of $13 million per year. They will also replace a wide variety of personal devices that its pilots have already been using.

Similarly we rarely find comprehensive risk assessments conducted for how the use of personal mobile devices might affect the overall risk profile of the enterprise. This is because the two primary drivers for their implementation commonly by-pass formal change management or assurance processes in place.

The first driver is from the bottom up. Staff will adopt practices and processes utilising the increased functionality offered in advance of corporate policy. This exposes the enterprise to increased information security risk without the ability to leverage the opportunities offered. Driven from the top down it may have approval from the board but will only deliver benefit to a small group within the enterprise.

A plethora of system monitoring and detection tools now exist to protect the increasingly diverse range of components that make up modern networks from a range of threats.

Most commonly we see top down initiatives introduced as 'trials' specifically to avoid controls in place to prevent such activity. These trials can last until the enterprise identifies a way for larger scale deployment which again can result in increased information security risk in conjunction with a limited realisation of the original opportunity.

The result is often a partial solution that delivers unsatisfactory results to both parties. While it may be more difficult and take a bit longer, following the formal enterprise route for introducing new technology can allow for the key points identified above to be addressed. It is unlikely all parties will ever be completely satisfied with the final result but at least there will be transparency in the process and a full understanding of the opportunities and risks involved.

For a more in-depth study of the risks and benefits offered by mobile devices please read Chapter 7, Mobile Devices.

Scenario 2: Using big data to secure the enterprise

A plethora of system monitoring and detection tools now exist to protect the increasingly diverse range of components that make up modern networks from a range of threats. These range from well-established anti-virus scans to specialised tools to detect evidence of cyber espionage attacks attempting to evade detection. These tools offer unparalleled insights into the operations and performance of networks. And they also provide risk officers the opportunity to deliver not just more effective network protection but also to enable the more efficient configuration and utilisation of network resources.

Enterprises are increasingly seeking to move from a reactive to a more proactive security stance to identify, investigate and remediate attacks before lasting damage is done. In many instances current Security Information and Event Management (SIEM) tools are hampering an organisation's ability to achieve this transition as they cannot effectively process the huge amounts of data now being collected from monitoring sources. Using big data in conjunction with effective and timely analytics can give risk officers a key tool in enabling this.

Automotive engineering and racing company McLaren Group place strategic importance on the protection of their information to exploit future opportunities for growth and innovation. McLaren uses a massively scalable platform to detect the underlying behaviours associated with sophisticated and bespoke cyber attacks, which typically go undetected and unfiltered by traditional methods that look for known attack signatures. This gives them the assurance at a time when the threat landscape and the impact of new technologies on IT infrastructure management is constantly evolving.

The ability to exploit the opportunities offered by big data is not without risks which include:

1. Scale: the cost of capturing, ingesting, processing and storing the vast volumes of security alert data becomes prohibitive; and

2. Effectiveness and Efficiency: unless correctly configured the sheer volume of security alerts generated, including false positives as well as low priority alerts can overwhelm analysts. Furthermore, unless there is an aggregation tool in place, capable of drawing together the various feeds, analysts will spend most of their time trying to connect the dots across different monitoring tools.

In order for risk officers to be able to truly embrace big data to help secure their enterprise it has to be in a way which overcomes the risks highlighted. When they find themselves hampered by an inability to efficiently process and analyse security alert data; with a corresponding impact that decisions are delayed or made on the basis of limited insight, it would indicate the enterprise is missing the significant risk management opportunities available to improve security.

Scenario 3: Connecting engineering and corporate networks

The practice of connecting previously disparate networks and systems together is becoming increasingly common in the enterprise. At a personal level there are apps available to enable smartphones to operate domestic lighting and audio systems as well as unlock and switch on vehicles. This scenario explores the opportunities and risks associated with connecting enterprise engineering and corporate networks, for example industrial controls systems.

Control networks and corporate IT networks are connected to improve efficiency, in controlling industrial control systems, responding to notifications and for the business information that can be collected from these systems. Efficiencies are realised through greater automation, centralisation and reduced associated overhead. From an enterprise perspective these make a compelling reason to pursue the opportunity. The opportunity crosses into two other scenarios: remote diagnostics conducted centrally can then be transmitted to mobile devices held by field staff; and big data collected from the engineering network can be used to better calibrate and understand the performance of the system.

Engineering systems have traditionally not been built with cyber security in mind. This was not an oversight or intentional omission, there was simply no need. The system was going to stand alone, use separate protocols and be operated by specialist staff. Security by obscurity was enough.

Connecting these systems to corporate networks that are connected to the internet has radically changed the risk profile that requires more effective risk management and mitigation measures.

In December 2012 Saudi Aramco, the national oil producer of Saudi Arabia was the victim of a targeted cyber attack. The attack successfully compromised the corporate network with the intention of traversing to the engineering production network and disrupting oil and gas production. While unsuccessful in preventing production it did wipe the hard drives of 30,000 computers on the corporate network.

Scenario 4: What the future might hold – the internet of things

The number of 'smart' or embedded devices is expected to increase to 50 billion by 2020[10]. There is no shortage of examples of ordinary consumer products that can now connect, and therefore be controlled, over the internet.

In many instances the opportunity to connect a device has trumped the risk of doing so and ensuring this risk is appropriately mitigated. One security researcher likens it to the mid-1990s when security was a distant thought of the designers and manufacturers[11]. This has a direct impact on the enterprise because many of these embedded devices are such commonplace items they are easily overlooked from an information risk perspective.

The opportunity, driven by user experience, is a seamless transition of data from and between devices and making it available to users regardless of their location or endpoint device. Picture the scene: you're editing your PowerPoint presentation for an important presentation before then checking on your daily electricity consumption at home and then remotely checking the fridge and ordering fresh milk. Incorporating this expectation into the enterprise clearly presents a myriad of risks. How long we have to work through these before it becomes reality remains to be seen.

In the meantime risk officers have to recognise it is not enough to merely deal with the mainstream technologies. A finger on the pulse of emerging technologies is also required. The internet of things will erode differences between the physical and logical, and the enterprise and personal even further. There remain a range of options to combat this from a risk perspective. A common theme through these is placing greater onus on individuals to take personal responsibility for information security. An education and awareness programme with a focus on concepts and practices that benefit the enterprise but are transferable to employees' private lives would be a good place to start.

Philips has manufactured LED light bulbs that connect to the internet and can be controlled via smartphone apps. It was quickly recognised by security researchers that the authentication method was vulnerable and could be easily compromised – allowing an attacker to switch lights on and off.

[10] http://blogs.hbr.org/2013/06/rethinking-security-for-the-in/

[11] http://www.darkreading.com/vulnerability/tackling-enterprise-threats-from-the-int/240161055

> Bring business opportunity management and information risk management together into the same room.

Conclusions and recommendations

Organisations need to bring business opportunity management and information risk management together into the same room. But balancing both is difficult. It requires three different skillsets: understanding of business strategy; knowledge of the technologies involved; and an understanding of the current threats. But the impacts of getting it right are significant and having an imbalance between the two can create significant damage. Too much focus on opportunity and the enterprise will be exposed to a level of risk in excess of tolerances; applying information risk management controls too tightly restricts the ability to successfully pursue opportunities. In summary:

- Ensure there is ownership and responsibility for risk governance and its interaction with opportunity management at Board level. This should then flow down the enterprise through management to the operational level allowing lines of communication both up and down the enterprise.
- A way to ensure an effective balance is to conduct regular risk assessments and receive regular key performance and risk indicators between these. These allow the board and senior managers to understand how the risk profile of the enterprise changes over time. It would also ensure the tolerance levels remain appropriate and that the corresponding control sets are commensurate to the level of risk faced.
- Where imbalances between risk and opportunities are detected, prompt remediation to address this will help ensure opportunities can still be pursued but in a secure manner.
- This normally entails recognising information risk management is not an IT concern to be addressed through technical controls. Rather, it is a business function that must be informed by the enterprise strategy, priorities and risk appetite. It also has to be flexible enough to recognise that risk appetite may vary with each opportunity identified.

The pace of technological innovation and the rapid evolution of industrialised cyber threats makes it all the more important to ensure an appropriate mechanism for recognising and responding to opportunity and risk is put in place. Paralysis in decision making can be the result or worse still the enterprise can expose itself to far greater risk while missing the opportunity to properly exploit the new industrial digital economy.

We have no shortage of examples where we have seen this situation develop, especially around the use of BYOD within the enterprise. Enterprises unable or unwilling to recognise and respond to new technologies can frequently find their staff adopting and integrating these into their working practices anyway. Adoption can increase the level of exposure of critical information assets to associated threats. It also means the enterprise has to try to retro controls, possibly harming their ability to pursue the opportunities these new technologies offer.

- Recognising the opportunities and risks associated with new technology is key to helping inform the enterprise response. A risk governance framework that is not suitably empowered or is imbalanced will struggle to ensure the enterprise responds in a timely and relevant manner.
- Lack of awareness among executives and the board to the issues presented by new technologies should be rectified as quickly as possible. A lack of understanding or knowledge could result in the enterprise adopting the wrong position or delaying a response until it is too late.

The digital economy will continue to pose new information risks and business opportunities for all organisations. The ability for an enterprise to thrive in the uncertainty of this brave new world will be influenced by their ability to recognise the opportunities presented and pursue them in a secure way.

> The digital economy will continue to pose new information risks and business opportunities for all organisations.

This chapter has been prepared by Applied Intelligence, a division of BAE Systems, formerly known as BAE Systems Detica.

Appendix 6.1

Key questions for the enterprise to ask in balancing risk with opportunity management.

Is the enterprise able to show they…

Are clear who is responsible	• Who on the board is responsible? • Who explains the risks to them? • On what information will we make decisions?
Understand their cyber risk	• What information is most important to us? • What types of cyber risk do we care about? • How exposed are we to those risks?
Make active decisions on risk	• What is our appetite for risk? • Have we communicated this to all functions? • Are our resources deployed efficiently?
Plan for resilience	• Do we cover "10 Steps to Cyber Security"? • How will we know we are being attacked? • How will we thrive despite attacks?
Support strategic priorities	• Does our risk mitigation facilitate and enable growth? • Are our controls delaying or blocking progress? • Are we agile enough to exploit market opportunities?

And common answers that indicate risk and opportunity is not in balance.

Are clear who is responsible	**Our IT department handles it**
Understand their cyber risk	**It is the same as everyone else**
Make active decisions on risk	**We do what we have to do**
Plan for resilience	**We need to stop them getting in**
Support strategic priorities	**Security is a burden for us**

> This chapter aims to provide guidance on the principles of assessing parties within the organisational supply chain that handle critical data."

Chapter 07: Cyber risk and the supply chain

Chapter 7: Cyber risk and the supply chain

Alastair Allison CISM SIRM

Do you have adequate control over the data that is critical to the business as it freewheels around the digital space inside and outside the organisation as you conduct business?

The Data Waterfall

One leading insurer mapped where its data went in respect of supporting one type of insurance claim involving personal sensitive data. The actual data transferred varied according to the need of the recipient. But typically it crossed several national borders and involved:

- 2 other insurers,
- 1 broker,
- 4 legal companies,
- 3 doctors,
- 2 police forces,
- Employer of the claimant,
- UK HMRC,
- A private investigator,
- the NHS,
- 2 courier firms,
- 1 engineering maintenance firm,
- a manufacturing company,
- and of course, the individual making the claim.

The insurer has in excess of 10,000 active claims being progressed at any one time.

Abstract

This chapter aims to provide guidance on the principles of assessing parties within the organisational supply chain that handle critical data. We outline the need for the process to be a risk based activity in accordance with the importance of the data an organisation holds and the risks to that data. We also highlight the key steps to an effective governance framework.

Introduction

Do you know who has your data or where your data goes? Verizon, in its 2013 report on data breaches in the US stated that 96% of breaches were attributable to outsiders with 9% involving multiple parties. Could you detect a breach before it becomes damaging? Again, Verizon reports that that 92% of breaches were detected by third parties and not the primary victim, so how good are your controls and your incident management processes within the supply chain? Do you know how any data item is shared to achieve the task in hand? (See "The Data Waterfall" box). Do you have adequate control over the data that is critical to the business as it freewheels around the digital space inside and outside the organisation as you conduct business? Experts stress that data security is a problem that requires an enterprise-wide solution.

[12] Critical data is any data that is essential to the operation of the business and provides it with a competitive advantage or is core to its operational role. It could be Intellectual property of designs or personal data of customers for the placing of insurance.

Case Study: Supply Chain Attacks

In February 2011, it was reported in the media that a cyber attack had occurred on the RSA Security division of the EMC Corporation where SecureID tokens were potentially compromised.

In May 2011, computerweekly.com reported that US-based global defence firm Lockheed Martin said it had beefed up security around remote access to its IT network after a "significant and tenacious attack" on 21 May, which could be linked to the breach at RSA. Lockheed Martin were building the stealth Jet fighters – designated F22 and F35.

In March 2012, British aircraft manufacturer BAE Systems confirmed that its systems had been hacked 3 years previously (2009) whilst they were working on the designs of the American F-35.

In February 2013, the first photos of the Chinese Shenyang stealth fighter aircraft, designated as the J-31, emerged on Chinese internet forums.

While there is no proof that China's latest stealth fighter stole design specifications from American stealth fighter projects, the Chinese jet appears to share many design characteristics of the American F-22 and F-35 jets.

IMPACT: Reputational damage and erosion of trust in partner organisations; potential loss of competitive advantage in certain markets due to exploitation of intellectual property; national security vulnerability.

An enterprise cannot outsource accountability.

"Monitoring must be multi-layered" to detect, prevent, and respond to threats that could be exploiting the weaker links in the extended enterprise.

"Data security and other cyber exposures are recognised as a significant threat by most risk managers, senior executive and board members of European organisations. These organisations are taking steps to manage the threats, but strategies and tactics vary widely" (Zurich/Advisen, 2013). Reports are rich in statistics but what does that actually mean for the risk management teams in organisations? Well, it suggests that having robust vendor diligence checks in place for Information security is crucial if the primary organisation is to be effective in managing the security of its data – it is not just about protecting the immediate business perimeter. It also means that organisations need to take control over the data they share. Another survey, this time by Experian/Ponemon Institute reveals that 46% of organisations do not evaluate the security and privacy practices of vendors before sharing sensitive or confidential information.

Often when enterprises outsource their activities, they think that when something has been outsourced to another enterprise, with a legally binding contract and monthly/quarterly relationship meetings, "the activity that has been outsourced will be looked after as they would have if they had not sent it elsewhere to be done" (Zarella). It is important to understand that an enterprise cannot outsource accountability. It is also important not to underestimate the risk simply because it has not happened to you. Experts noticed that companies sometimes "forgo investment in security because it has not yet harmed their organisation or because they mistakenly believe that they have nothing a cyber adversary would want. More importantly, they misunderstand that their own cyber insecurity has collateral effects on others – effects for which they are responsible" (Bucci, Rosenweig and Inserra). With such prevailing attitudes, it is crucial for organisations to recognise the cyber risks across the extended enterprise and develop risk mitigation strategies to deal with them.

The Risks

"While many companies report success at maintaining internal cyber security, their links with other organisations—particularly suppliers, as supply chains grow longer and more complex—are less easy to manage" concluded a Harvard Business Review into Cyber Security. "Monitoring must be multi-layered" to detect, prevent, and respond to threats that could be exploiting the weaker links in the extended enterprise. However, we do not want to leave the impression that the use of suppliers inevitably increases the organisational risk. Far from it, the use of third parties or outsourcing work does not in itself increase the risk but poor processes within the external party and poor governance do. The 2013 Verizon report highlighted that 97% of breaches were avoidable and it is suggested that inadequate attention to the risks may have contributed to potential breaches being overlooked. Risk analysis is the first step toward better protection.

Cyber risks could result in:

- Loss of intellectual property including designs or strategies for market penetration resulting in loss of competitive advantage.
- Loss of customer data, or access to and disclosure of, customer data outside of business policy.
- Instances of losses of customer data, or access to, and disclosure of customer data outside of policy which are not identified and addressed appropriately.
- Inadvertent use of personally identifiable data to support big data analytics leading to a regulatory breach or harm to individuals.
- Industrial espionage to undermine business critical operations, investments or mergers and acquisitions.
- Regulatory non-compliance
- Distress to customers and individuals
- Damage of organisational reputation
- A loss of market share
- Adverse share price fluctuations including deliberate short-selling after manipulation of company reputation.

The Data Breach Trail

A global company reported that they were contacted by an individual claiming to have over 10,000 of their customer records and offering to sell it back to them before it went on the open market. The company were able to verify the data was theirs and that it had originated from one of their suppliers.

The company immediately set up an incident response team and found that a rogue employee within a supplier had stolen the data (due to weak controls) and had passed the data on for re-sale. The data, including customer data from nine other companies in the same sector, had passed through hands in three countries. At least six other marketing companies had bought the data believing it to be legally obtained.

Within the first week the global company took out three injunctions in three different jurisdictions and ensured its supplier took every measure to limit the spread of the data to the market and seek full recovery. In its subsequent follow up work, the Global company belatedly found over 23 weak security practices in its third party's operations. Earlier due diligence and better governance would have exposed these weaknesses.

The regulators were informed early in the process and it was only the swift and extensive action taken to recover the data that prevented a fine being levied. The company did not pay for the recovery of the data.

The Benefits

As large international organisations make it more difficult for cyber criminals to make a direct attack, the evidence suggests that smaller companies become more attractive to cybercrime if they process the right sort of data. Effective governance of third parties is, therefore, essential to data security. The scale of the oversight operation will need to be commensurate with the risk and the size of the organisation. The benefits, however, should not be under-estimated. The largest benefits of supply chain oversight is that the virtual barriers are pushed even higher and further away from the organisation thus protecting its reputation and that the supply chain as a whole becomes ever more resilient.

The increasing regulatory pressure on organisations adds a dynamic flavour to the risk process. However, oversight of the supply chain not only makes good sense, it also benefits organisations by protecting future competitive advantage and, therefore, protecting the customer base and their trust in the organisation. Additionally, it:

- Ensures business critical data is secured in accordance with contract and regulatory requirements.
- Ensures compliance with contract terms and conditions including pricing and discounts, KPI/SLA penalties and management of P&L etc.
- Leads the resolution of local performance issues at an appropriate level and allows for escalation to business managers as required.
- Steers negotiation efforts at process development and renewal phases.
- Ensures that the supplier delivers services in a way that enables the organisation to meet its regulatory obligations.
- Ensures adherence to organisational policies, guidelines, values and brand.

By exercising proactive oversight of the supply chain, organisations are better able to control their own destiny and costs according to the business risks they face rather than operating according to the timetable of a regulator following an imposed supervisory order in the event of a breach.

Cyber risks in the extended enterprise – should we be concerned?

"Printers who specialise in direct mail projects are often amazed by the amount of very personal data in the file that comes from the customer. The promise of variable data printing is still under-served around the globe, but the possibility that the data file contains everything from credit information to social insurance information is real. In other words, far more than is necessary to execute a personalised direct mail campaign."

Kevin Keane (President and CEO –
IAPHC Inc., (USA)
Contributing to a LinkedIn discussion

The increasing regulatory pressure on organisations adds a dynamic flavour to the risk process.

The Challenge

The supply chain can become large for many organisations. One company reported they had over 6000 suppliers and they had assessed the information security risk each presented to its business and that they would apply differing levels of supplier management and oversight according to that risk. They also expected their third parties to do the same and exercise sufficient oversight and management of their third parties.

THE IRM RISE Special Interest Group cyber risk survey noted that over 45% of respondents did not review information security practices of a potential supplier prior to contract award, thus leaving a significant gap in the governance of the supply chain. Furthermore, business units within organisations may have procured services outside the normal procurement process and these suppliers may go undetected from a cyber-risk review perspective. Nevertheless, it is essential to assess whether these organisations have recognised that they remain accountable for their information exchange operations even when they have outsourced the function. The size of the supply chain is clearly a key challenge for many organisations but the need to develop effective governance and oversight controls is essential. Additionally, organisations must also challenge the need to send critical data in the first place and remove any data not actually required by the recipient (see box opposite).

Another factor is that smaller organisations today are more likely to use cloud computing technology (Zurich/Advisen). The IRM survey showed that over 90% of respondents permitted the use of mobile devices such as smartphones and tablets yet 53% of respondents failed to use security applications to control data security on such devices. With this in mind, it is essential for organisations to ensure that such technology within their supply chain does not inadvertently leak sensitive data to the public cloud or allow it to be extracted though a third party application.

The agility of smaller suppliers will increase the risk of data leakage if they do not have robust risk management practices in place. A state of "data anarchy" may well be present whereby data is not classified and flows freely around the internet and cloud solutions (such as Drop Box) without any controls in place. Data will be beyond effective control of the organisation and could result in serious financial consequences. Data anarchy could well exist within third parties unless there is sufficient oversight from the contracting party. Consequently, if an organisation has not conducted reasonable due diligence to take adequate technical and procedural measures for the protection of the data it transfers, it may be in breach of regulatory requirements that could result in fines at a time when the power to hand out greater fines is growing.

The Key Steps

There are certain key steps to ensuring supply chain cyber security practices are effective and these are outlined below.

- Devise a risk and cyber supply chain governance framework including risk tolerance
- Identify critical data being shared across the supply chain and its value to the organisation
- Educate (internal and external)
- Review contract wording
- Undertake due diligence activities
- Monitor performance during the contract
- Implement an escalation process
- Ensure effective evidence gathering
- Ensure effective incident reporting processes.

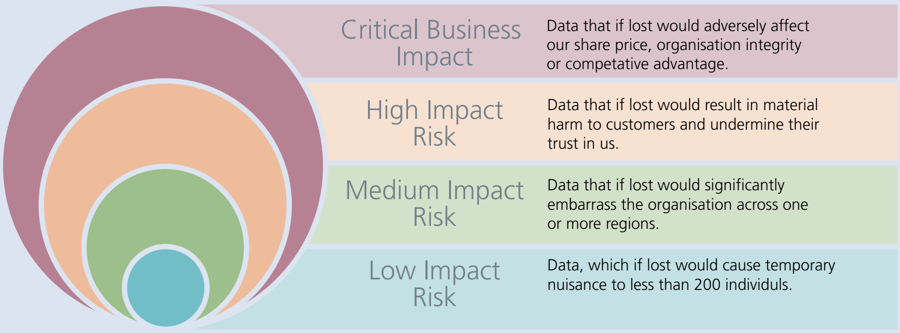
However, even if all these steps are taken, they can provide no guarantee against the activities of individuals or staff at suppliers who might commit malicious activities or are prone to human error.

Devise the Governance Framework

It is essential to determine how cyber risk in the supply chain is to be governed so that all subsequent processes are measurable and justifiable and to prevent over-committing resources. As far as possible this should fit into existing processes. It could involve simply verifying the state of the supplier's cyber environment annually through a self-assessment questionnaire such as the one at Appendix 7.1 or it could become part of the wider organisational due diligence processes.

In essence, a governance framework is required to provide oversight of the supply chain risk, determine the policies and procedures and ensure the risks are being managed to within the organisational tolerance limits. Clear roles and responsibilities need to be defined including who has ultimate responsibility for each supplier (Contract Owner) and who manages the supplier relationship on a day-to-day basis (Contract Manager).

Figure 7.1: Risk Criterion Table



Critical Business Impact	Data that if lost would adversely affect our share price, organisation integrity or competative advantage.
High Impact Risk	Data that if lost would result in material harm to customers and undermine their trust in us.
Medium Impact Risk	Data that if lost would significantly embarrass the organisation across one or more regions.
Low Impact Risk	Data, which if lost would cause temporary nuisance to less than 200 individuls.

> It is essential to determine how cyber risk in the supply chain is to be governed so that all subsequent processes are measurable to prevent over-committing resources.

The governance process should consider the business impact of a data loss against its risk appetite and set the risk parameters as shown in the example at Figure 7.1. In terms of certain data types, such as medical data or personal sensitive data, the risk appetite will be shaped by the regulatory environment which may also prove useful in determining quantitative thresholds for the number of records involved or the sliding scale of financial penalties in the event of a breach. Again, this should fit into the organisational risk process and allow for effective reporting of risks that are above threshold.

The governance process surrounding the supply chain risk posed from cyber threats should cover the normal governance areas including the determination of values and behaviours, measurement and effective oversight so that timely intervention can be made to prevent an issue becoming a crisis. Such a review can be aligned to particular standards or guidelines that the organisation is using such as ISO27001, as listed below.

1. Security policy
2. Organisation of information security
3. Asset management
4. Human resource security
5. Secure areas
6. Communications and operations management
7. Access control
8. Information systems acquisition, development and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance with legal requireents

With the governance framework in place to allow effective and risk based oversight of the supply chain, it is essential to map the key governance requirements to the risk threshold diagrams so that the contract owners/managers can clearly see the relationship between what they are doing with the risks to the organisation. For example, Figure has been used to drive the high level due diligence reviews that will be required.

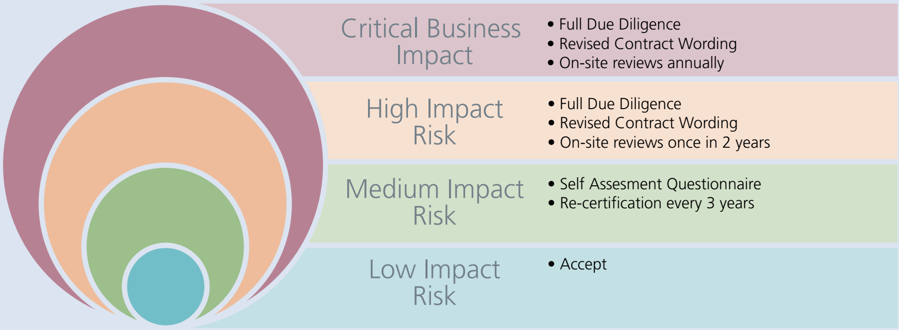
Identify that Critical Data

There are two steps to identifying data critical to a business. The first is to identify the types of data that are critical to the business and the second is to identify where it goes outside the organisation.

Such data could be designs, floor plans or requirements for bespoke systems that give competitive advantage or it may be customer records.

What will help the identification is a data classification system so that the most sensitive data is identified separately from publicly available data. It is good practice when an organisation can identify data according to the criticality of it to the business. For example, an organisation may classify any data that could affect its share price, such as unpublished financial results, as TOP SECRET. If that organisation has outsourced its printing operations to a third party, those results will leave the organisation to be printed and subsequently returned to head office for release and distribution. The classification level can be used to determine the level of protection during transit and handling and also any contractual requirements such as confidentiality clauses. Consequently, data classification permits the control environment to be designed according to the risk to the organisation rather than taking a one-size-fits all approach. It also then allows suppliers to be ranked according to the classification of data they process and, when combined with an understanding of the volume or frequency of data exchange, can be used to tier the suppliers.

Figure 7.2: Risk Mitigation Strategies



Critical Business Impact	• Full Due Diligence • Revised Contract Wording • On-site reviews annually
High Impact Risk	• Full Due Diligence • Revised Contract Wording • On-site reviews once in 2 years
Medium Impact Risk	• Self Assesment Questionnaire • Re-certification every 3 years
Low Impact Risk	• Accept

Data components will depend upon the data being protected.

Filtering can then be applied to the list of suppliers to identify the key suppliers so that those that process no data can be filtered out. The criterion for filtering suppliers could be based on:

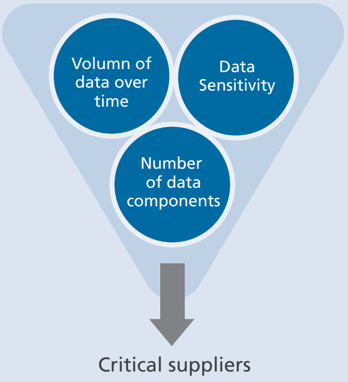
- the volume of data,
- sensitivity of the data and
- the number of data components (name, address etc.).

With data components, the actual number that are shared compared to the whole picture will give a measure of the risk that a competitor could gain advantage from IP theft or a data loss. Data can be assessed by being put through a filter so that, for example, only those with high sensitivity (medical records or high net worth IP) are classified as high risk.

Data components will depend upon the data being protected. For system design for example, the more complete the design specifications are to the end product the easier it is for others to assemble that new product and get to market. For personal data, it is widely accepted that only five key pieces of information are required for identity theft. Consequently, any data exchange involving five or more pieces of such data poses a greater risk than anonymised data particularly if that data is unencrypted.

As no organisation has the resources to conduct on-site reviews of all its suppliers, filtering is an attempt to create a risk based approach to supply chain oversight. It also aims to shape a governance model by understanding the scale of the task involved. Using Figure as our example, the filtering for the current supply chain could be extended as shown opposite to create three tiers of suppliers. However, other companies may be further filtered out if an independent cyber-review had already taken place in the last 12 months and there were no additional services added since the last cyber-review. Thus, it would be easy to create a tiered view of the supply chain

Figure 7.3: Critical Supplier Identification



Education is a critical part of supply chain management.

that allows resources to be directed at the highest risk areas. This might look like the following:

- Tier 3 – Low risk organisations that share data but with a narrow number of data components that of themselves, do not constitute a threat to customers if the data was lost. Self-assessment surveys issued every three years.
- Tier 2 – Medium risk organisations that directly support core business but with smaller volumes of data exchange and lower sensitivity of data. These require less oversight and on-site visits required every second year only.
- Tier 1 – High risk organisations that directly support core business and require annual oversight with on-site visits and quarterly performance reviews.

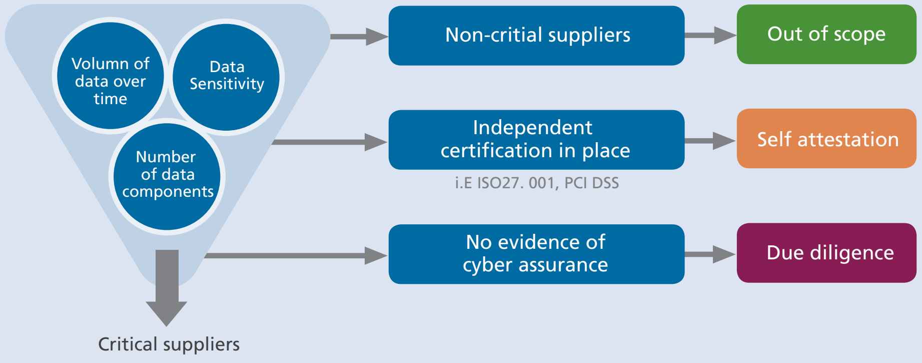
As Bayuk outlines in his ISACA article, the use of scenarios as an approach to vendor due diligence is a useful tool. He outlines the following five scenarios for organisations to consider:

A. The firm compiles a list of questions intended to identify control activity that would support business requirements. The vendor fills out the questionnaire. Where vendor answers do not match requirements, this is reported.

B. Same as scenario A, but in addition, the vendor is interviewed via telephone or e-mail to explain questionnaire answers and provide evidence of alternative controls.

C. Same as scenario A, but in addition, where vendors are considered high risk, the firm visits the vendor site to verify answers and clarify responses.

Figure 7.4: Diligence approaches after filtering



D. The firm reviews the vendor data processing environment by charting the path taken by data in scope. The vendor is requested to provide documented evidence of controls. The firm confirms its understanding of the vendor environment via phone interviews.

E. Same as scenario D, but in addition, where vendors are considered high risk, the firm performs or requires independent verification of controls, to include Internet scans, onsite audits and/or reports of independent auditors.

Regardless of the methodology chosen, it is clear that all organisations have limited resources for assessing the adequacy of the supply chain. Furthermore, the need to classify data and assess the exchange of such data not only applies to the existing supply chain but also to new contracts. Such an exercise can be used to determine the level of controls that should be implemented as part of contract award. For example, if the contracting parties are to exchange personal or personal sensitive data on a daily basis then it may be necessary to put secure email solutions in place. If the parties will be exchanging intellectual property involving design specifications then a secure operating environment in a private cloud solution may be required.

Education

Education is a critical part of supply chain management. Indeed, the act of conducting due diligence and working with the supply chain to resolve the issues is part of that education process. An organisation embarking on supply chain evaluations should first train internal staff to be competent in conducting such evaluations so they can ask the fundamental questions and understand the implications behind the responses.

Light touch approaches that rely on suppliers responding to critical questions or to provide evidence of accreditation to a specific standard still requires someone to assess the responses and make a judgement on behalf of the business. On-site reviews require a different level of competency and a certain amount of legal awareness if liabilities are not to be inadvertently transferred between parties. Each role involved in the evaluation process needs to be examined and training performed where appropriate.

A contributor to this research stated that they provided a one day training course to over 70 of their contract managers on how to plan, conduct and assess the outcomes of on-site reviews including what constituted good evidence, and what typically to watch for when conducting a cyber-review. The training allowed the contract managers to dig deeper, assess the evidence and to challenge the responses so that they were able to make a firm recommendation to the business on whether or not to trade with that supplier. As non-specialist staff, they were not only provided with the training and appropriate toolkits but they also had support from subject matter experts to deal with the more challenging technical and procedural aspects of cyber security that only experience and specialist knowledge can provide.

We recommend that organisations reserve rights in contract to undertake reviews, penetration or vulnerability tests or other work during the course of a contract.

Review Contract Wording

Contract wording is important when trying to build a layered defence for better cyber security practices. There needs to be a clear articulation of what constitutes the critical data to be protected, the data risk and the method by which data is to be classified and subsequently protected that adequately covers the data regulation environment. This must take into account the different territories that the data will transfer to and be stored within. Where applicable, the contract should include the minimum security standard to be applied and define the agreed level of encryption and/or data transfer methods. It should also consider how data is to be retrieved at termination of the contract. Organisations that do this tells us that they include the minimum standard in the contract negotiation phase and negotiate on the latitude to be afforded to data security in light of the services and data transfers that are to occur. If this is all agreed from the start of the contract then control will be easier to maintain.

Additionally, the contract needs to be explicit in stating the incident reporting obligations for both parties including timeframes. Emerging regulation is putting pressure on organisations to report to regulatory bodies sooner and with more detail. Such requirements need to be cascaded throughout the supply chain.

We recommend that organisations reserve rights in contract to undertake reviews, penetration or vulnerability tests or other work during the course of a contract. This will include rights of action in respect of an incident or regulatory review. This may be resisted, especially by cloud service providers, but efforts must be taken to allow investigation and inspection.

Due Diligence Activities

Zurich Insurance Group, when trying to determine its preferred approach to supply chain due diligence for cyber security, commissioned a piece of research with KPMG[13] to understand what the rest of the sector were doing in this space in 2009 (the year the report was commissioned). The results in Table 7.1 – Comparison of Due Diligence activities in the Financial Services Sector highlight six methods that could be adopted either singularly or combined depending upon the overall governance model adopted and aligned with the Bayuk scenarios outlined previously.

[13] Table and contents are kindly provided with permission from Zurich Insurance Group (UK General Insurance) and KPMG.

Table 7.1: Comparison of Due Diligence activities in the Financial Services Sector

	UK based global bank	UK based global financial institution	UK financial institution	Global card payment organisation	US based global financial institution
Number of high risk third party suppliers	800 ('08/'09)	100-250	250+	300	50-100
No of third party security reviews planned for 2009	800 ('08/'09)	100-250	100-250	300	50-100
Number of third party security reviews planned for 2010	Unknown	50-100	250+	300	50-100
Self-assessment	No	Yes	Yes	Yes	Yes
Telephone interview	Yes	Yes	No	No	No
On site assessment	Yes	Yes	Yes	Yes	Yes
Base questionnaire	Bespoke by client	Bespoke based on ISF	ISF	Bespoke aligned to PCI DSS	Bespoke aligned to BITS
No of days on site	1	1-5 & 5-10	1-4	4	2

It is clear that there is no "one-size fits all" approach and each organisation will need to determine what is appropriate for it to do given the risk and the resources available. It will also be necessary to determine the level of training required to support the process. However, the conduct of due diligence prior to contract award is the right thing to do. Of course, many organisations also have a large supply base already in existence so taking the above for guidance, due diligence on information security capability should be conducted retrospectively according to the risk presented as described above although agreeing a remediation plan may require further negotiation or possibly renewal of the contract depending upon the severity of the findings.

Due diligence is normally associated with new contracts so it is essential that business as usual processes are devised to keep abreast of the changing landscape and that the supply base responds to the changing risk context. This is best achieved through the performance monitoring processes.

Monitor Performance

Due diligence for information security and cyber risks is likely to be a one-off exercise at the beginning of a contract or at contract renewal but continued compliance with the contract terms, service level agreements and performance metrics will need to be monitored in a business as usual approach. For this to occur, performance management needs to be embedded into other due diligence or contractual review processes so that the data security risk remains in context with the other business activities being performed.

The following need to be in place:

- Updating of the risk assessment of the cyber environment
- Regular risk reporting against other suppliers
- Evidence of proportional oversight activities according to the risk
- Escalation of any data security breaches to the appropriate internal team charged with managing such issues.
- Regular relationship meetings with any actions recorded, agreed and resolved.
- Assessment/monitoring of emerging, new and existing risks
- Review of the progress against remediation plans from audits/due diligence work.

Tracking of remediation work is essential if gaps and vulnerabilities are to be closed down in a timely manner. As with all reporting, it needs to be tailored to the organisation and the detail tailored to the audience. For example, details on each remediation action for a single company is appropriate only to that company or the team charged with ensuring actions are closed down. Management require oversight of all the companies and the total plans outstanding whilst the risk and compliance team may just need to know that annual inspection plan is on target and that actions are being appropriately managed and escalated. Appendix 7.2 provides some examples that could be used to achieve performance reviews dedicated to information security.

Escalation process

Of course, not all suppliers in the chain will wish to accommodate remediation actions as it will no doubt add costs to the service they provide. Even with increased regulatory pressure to safeguard personal and personal sensitive data, some organisations will resist any action that adds costs to their business. It is essential, therefore for organisations to have clearly defined escalation procedures that can lead to the appropriate decisions being made to manage the risks as they present themselves.

Figure 7.5 – Escalation Process highlights four potential scenarios and what escalation processes may need to happen, including the option of terminating a contract. This is not always possible as a supplier may be the only source of a product or service or the industry standard is such that the proposed changes will put them at a commercial disadvantage within their sector. In such cases it may be necessary to accept the risk. If this is the case, full documentation should be kept of the decision and the rationale for it in case it is required for internal review and potentially for regulatory purposes in the future. Notwithstanding this, if organisations are to take cyber security seriously and enforce the same approach in the supply chain, they must be prepared to make hard

> Tracking of remediation work is essential if gaps and vulnerabilities are to be closed down in a timely manner.

commercial decisions even if there has been a long term relationship. Data security is no longer a risk than can be readily accepted or ignored. It has to be proactively managed across the extended enterprise and for some, it may mean that the cultural fit now has to be challenged.

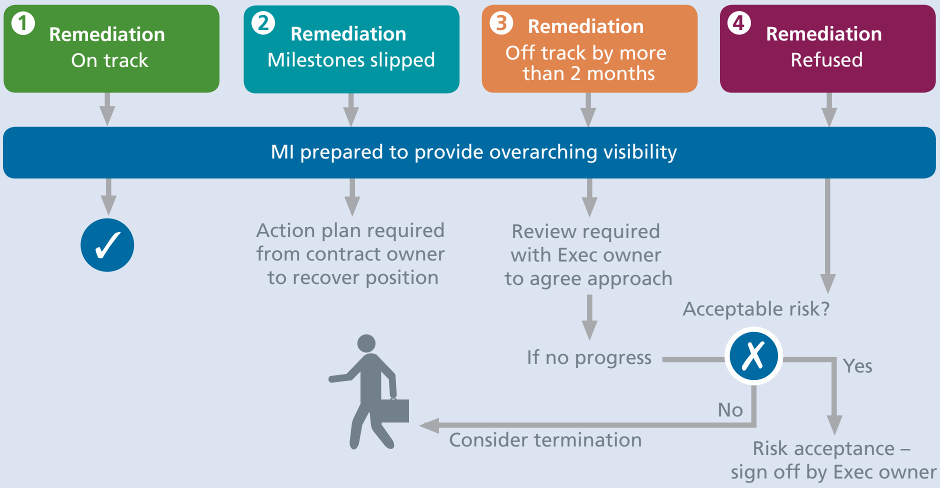
Evidence

Supply chain governance requires accurate and up to date business evidence to be maintained of all phases of the process (including post-contract). These documents provide a complete audit trail of decision making, data evidence, signature, risk assessments etc. in the event that a data breach does occur and the oversight of the supplier is called into question. This does carry its own risks and organisations will have a duty to ensure that all evidence is securely stored, classified and retained for the correct retention periods. Evidence is essential to also compare one year with the next and spot trends.

Ensure effective incident reporting

Devising an incident reporting process that is risk based with pre-defined severity levels and takes into account the regulatory reporting requirements is essential. In some jurisdictions and/or industries there is a mandatory requirement to report information security breaches and it is important therefore that processes and contracts are in place with third parties to ensure this occurs. It is also important that proportional responses are made in respect of any breach to prevent undue escalation and setting off time consuming and costly activities that are not required. If the incident can be handled appropriately at a local or junior management level then it should be.

Figure 7.5: Escalation Process


1 Remediation On track
2 Remediation Milestones slipped
3 Remediation Off track by more than 2 months
4 Remediation Refused
MI prepared to provide overarching visibility
✓
Action plan required from contract owner to recover position
Review required with Exec owner to agree approach
Acceptable risk?
If no progress
Yes
No
Consider termination
Risk acceptance – sign off by Exec owner

There are many and varied risks to the security of data shared across the extended enterprise and the attack vectors and scenarios are increasing in complexity.

If there is a serious risk of regulatory or reputational damage, then escalation to organisational executives will be a priority. Clearly defined escalation criterion with roles involved will remove ambiguity in the event of a crisis when people do not always work at their best. Additionally, it should be established whether the primary organisation will lead the investigation or if it is to be a joint process and, in the case of regulatory reporting requirements, what information should still flow between the organisations notwithstanding the requirement to report breaches directly to regulators.

Although response details are tailored to each situation, the response to any incident must include the following key objectives:

- Conduct a risk assessment
- Contain the breach
- Recovery of data
- Communication and notification to appropriate stakeholders/customers
- Investigation of the incident
- Improvement mechanisms to be identified including addressing the root cause.

This list should not, however, be considered as a linear process. The first 2 bullets, for example, often happen in parallel. Organisations should look to address the root cause and, at some point in the following 12 months, verify that the planned improvements have been implemented and are still operating in a business as usual environment.

Conclusion

There are many and varied risks to the security of data shared across the extended enterprise and the attack vectors and scenarios are increasing in complexity. Conducting due diligence of the cyber security capabilities across the extended supply chain is growing in importance particularly as any organisation is only as strong as its weakest link.

Organisations need to consider what their data "crown jewels" are and the risks they face in the event of a data breach/loss and take steps to protect the organisation by developing a robust supply chain governance framework. That framework will require training and awareness of key staff to enable effective monitoring of performance. The investment can often mean better decision making about whom to trade with and over the control of data to the point of eliminating data transfer risks.

It will be important, in the event of a breach, to be able to demonstrate to regulators and stakeholders that the organisation has been proactive and taken a risk based approach to managing the data flows across the extended enterprise and that incidents are handled well. In this digital age, a quick, appropriate and proportional response to an incident can make all the difference in how the media comment upon the organisation all over the world. Improving operational resilience across the supply chain may also prevent the need to test any incident response plan.

Reading list and websites

1. Bayuk, J, 2009 *Vendor Due Diligence ISACA Journal Volume 3*
2. Bucci, SP, Rosenweig, P and Inserra D, 2013, *A Congressional Guide: Seven Steps to U.S. Security, Prosperity, and Freedom in Cyberspace* accessed on line at **http://www.heritage.org/research/reports/2013/04/a-congressional-guide-seven-steps-to-us-security-prosperity-and-freedom-in-cyberspace** on 8 April 2013
3. *Case Study of the Chinese Fighter jet* accessed via **http://killerapps.foreignpolicy.com/posts/2012/10/31/chinas_newest_stealth_flighter_flies** on 22 Mar 13
4. Experian/Ponemon Institute, 2013, *Securing Outsourced Consumer Data*, accessed via Experian Website, **http://www.Experian.com/ConsumerDataStudy** on 4 April 2013
5. IRM, May 2013, *Cyber Risk Management Survey*
6. ISACA, 2002, *Effect of 3rd Parties on an Organisation's IT Controls ISACA Journal Volume 4*
7. ISO 31000:2009 – *Risk Management Principles and Guidelines*
8. ISO/IEC 27001:2005 – *Information Technology – Security Techniques – Information security Management – Requirements*
9. The Business Continuity Institute website **http://www.thebci.org/**
10. Verizon, 2013, 2013 *Data Breach Investigation Report*, accessed via **http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf**
11. Zarella, E, 2008, *You Can't Outsource Control ISACA Journal Volume 6*
12. Zurich/Advisen, 2013, *2nd Information Security & Cyber Liability Risk Management Survey,*
13. Zurich, 2013 "*Meeting the Cyber Risk Challenge"* Harvard Business Review

Appendix 7.1 – Due diligence questions – an example

The following table aims to be a compromise between a superficial review and the more detailed question sets used by some contributors to this research paper involving in excess of 150 questions. It provides a list of questions that might typically be used to assess the effectiveness of a third party cyber environment. Organisations wishing to use this list should integrate it into a risk assessment based on the level of good practice observed and an assessment of the vulnerabilities and threats resulting from any gaps as described further below. An alternate approach is to have closed questions only where by the "No" responses are all highlighting the gaps but the responses, whilst easier to provide and total up, can mask a multitude of sins unless all ambiguity is removed.

Cyber security due diligence review	
	1. Who is responsible for the day to day security within your organisation?
	2. Who do they report to?
	3. How is security managed within your organisation?
	4. How are risk assessments communicated and how is sign off obtained from the key stakeholders within the organisation?
	5. Where is your information security policy?
	6. How is this kept up to date?
	7. How do you know people have read the policy?
	8. Do you test staff understanding of data security policies on induction and once a year after that?
	9. Does your policy include any specific notification requirements if there are incidents in relation to organisational information?
	10. Is there an emergency response process for dealing with serious security incidents and attacks?
	11. How do you classify information within your organisation?
	12. How do you classify organisational information?
	13. Do you know where all information is stored within your organisation? How?
	14. What policies, procedures and practices do you have in place for secure transfer of customer and sensitive data?
	15. How do you keep track of all your IT hardware and removable media?

	16. What is your destruction policy for hardware, removable media and paper documents?
	17. What aspects of information security are included in your T&Cs?
	18. Can you take me through your access management process?
	19. Who is responsible for informing IT about leavers and joiners? Can you talk me through your process?
	20. What checks apply prior to the appointment of temporary staff and contractors?
	21. How are all new joiners including temporary staff and contractors made aware of your security policies?
	22. Are there any additional measures taken to vet those staff with access to customer data either on appointment or on promotion/change of role?
	23. How do you inform staff of changes or updates to the security policy?
	24. How are temporary members of staff made aware of your security policies?
	25. How do you control access to the building?
	26. What is your procedure for visitors?
	27. How do you control access to secure or sensitive areas?
	28. How do you protect your back-up tapes and who is responsible?
	29. Can you describe the process around transportation of data for backup / destruction – is the data encrypted?
	30. Can you describe the process for the destruction of hardware, removable media and paper documents?
	31. How do you protect your sensitive areas or key services from fire or flood?
	32. Do any of your suppliers or their suppliers manage or have access to organisational data/ systems?
	33. How do you manage / monitor those suppliers?
	34. How is access to organisational data controlled?
	35. Describe your controls in place in regards to anti-virus, anti-spyware and intrusion detection software?
	36. How do you ensure that this software is always containing the most up to date protection?
	37. How often is a full scan of workstations and servers performed?
	38. What processes are in place to make backups of your systems holding and processing organisational information?
	39. Where are back-up media stored on-site? What is the retention period on-site?
	40. Do you store back-up media off site?
	41. Do you outsource storage to a third party?

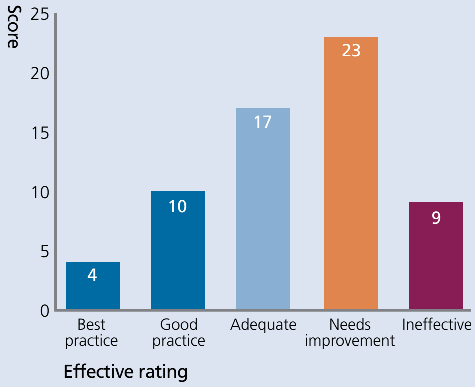
	42. Do you have an inventory of back-up media stored off-site?
	43. Do you have a data inventory for all classified data?
	44. What exceptions to information security policies and procedures are in place and what controls are in place addressing any additional risk?
	45. If anyone is responsible for storing back-up media at their home, do you provide a safe?
	46. Can staff access social media, Facebook etc.? Can staff access their email via web applications?
	47. Are there controls in place that monitor the appropriateness of data leaving the network?
	48. Do you scan the content of email attachments going out?
	49. Do you have any wireless networking facilities at your sites?
	50. If yes – what security mechanisms are in place to prevent unauthorised access to organisational information over wireless (e.g. authentication mechanism, encryption, firewall segregation from main network)?
	51. Who is responsible for controlling laptops and removable media?
	52. Do you have a formal IT asset register, or if not, as an alternative do you have a formal list of your critical assets which hold organisational information?
	53. How often do you carry out independent testing of your internet facing applications?
	54. If you develop your own bespoke applications how do you test them before going live? What data do you use?
	55. How do you monitor access to organisational information or to secure areas?
	56. How would an individual member of staff report a security incident or event?
	57. What events or incidents are required to be reported?
	58. Have any of these incidents occurred in the last 12 months?
	59. Is any organisational data stored or replicated for BC & DR purposes? Describe the security controls around this data?
	60. How often does your internal audit check the organisation compliance with information security policies?
	61. What independent assessments are you subject to SAS70, PCI, ISO27001 etc.?
	62. What training takes place with regard to information security and how many staff have received this in the last 12 months?
	63. Do you have agreed procedures in place with your third party suppliers in regards to reporting data security breaches within an agreed timeframe?

Each response to the above could be rated according to a predefined scale which in turn could be used to drive an objective risk rating to compare one party to another. One scale might include; Best Practice, Good Practice, Adequate, Needs Improvement, Ineffective.

Thus, a completed assessment would look as indicated in the diagram below:

Question	Effective Rating
1. Who is responsible for the day to day security within your organisation?	Adequate
2. Who do they report to?	Best Practice
3. How is security managed within your organisation?	Adequate
4. How are risk assessments communicated and how is sign off obtained from the key stakeholders within the organisation?	Ineffective
5. Where is your information security policy?	Needs Improvement
6. How is this kept up to date?	Ineffective
7. How do you know people have read the policy?	Best Practice
8. Do you test staff understanding of data security policies on induction and once a year after that?	Ineffective
9. Does your policy include any specific notification requirements if there are incidents in relation to organisational information?	Needs Improvement
10. Is there an emergency response process for dealing with serious security incidents and attacks?	
11. How do you classify information within your organisation?	
12. How do you classify organisational information?	
13. Do you know where all information is stored within your organisation? How?	
14. What policies, procedures and practices do you have in place for secure transfer of customer and sensitive data?	
15. How do you keep track of all your IT hardware and removable media?	

The results can then be compiled to give a view of the risk landscape as follows:



3rd Party Assessment

Best practice	4	6.3%	49.2%
Good practice	10	15.9%	
Adequate	17	27.0%	
Best practice	23	36.5%	50.8%
Ineffective	9	14.3%	
TOTAL	63	**Overall risk assessment**	**High risk**

Appendix 2 – Tracking the remediation plans – an example

Tracking remediation by company

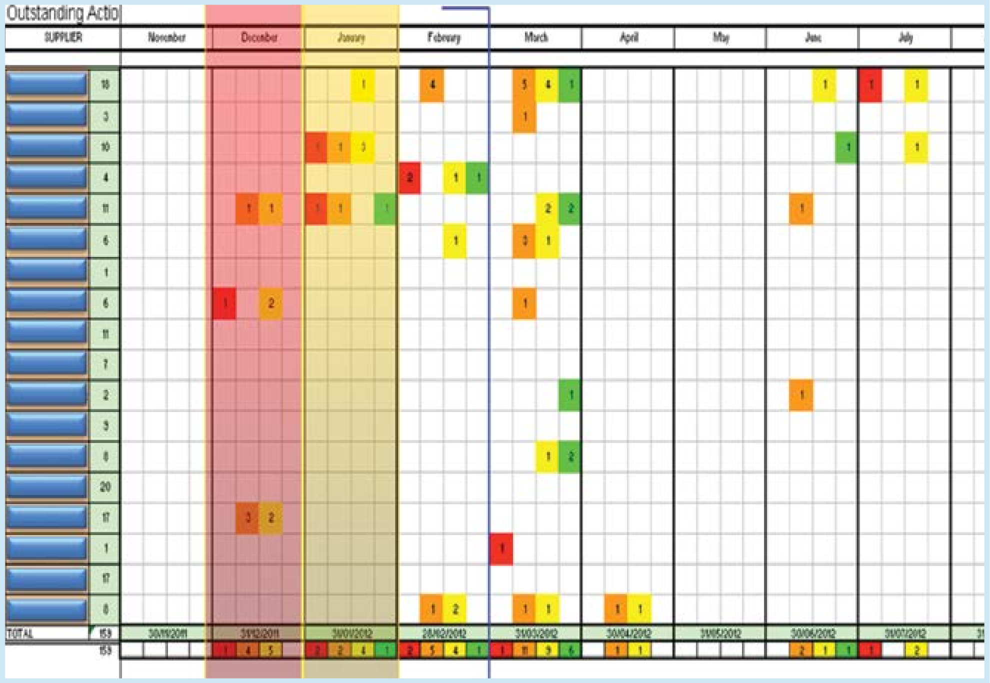
It is recommended that a template is prepared that allows consistent reporting of information security capabilities in the third parties that cross refers to the question set issued so that cross referencing can occur. The report should cover the following headings/fields and is probably easiest to manage within a spreadsheet:

- Reference Number (i.e. question number from the issued due diligence questions)
- Review finding
- Recommended action by the contracting organisation
- Agreed action(s) between the parties
- Status (i.e. red, amber or green)
- Start date
- Due date
- Actual delivery date
- Issues raised (for use at intervening periods prior to delivery date)
- Issue resolution
- ISO 27001 or other such standard mapping (i.e. refer to a control reference number)
- Supervisor's comments.

Management tracking and oversight

Tracking the remediation of a number of companies will require a mechanism that allows for the risk to be assessed as well as manage the closure of the risks. One method is a simple spreadsheet list with a number of actions noted against a closure date as shown in the diagram below. This shows the severity of the risk attached to each remediation action and which month they are due to be completed. "Time Now" is annotated with the blue vertical line whilst the yellow and red areas show those actions that are greater than 30 or 60 days overdue respectively. At the base of the table is the total number of actions due per risk rating which in this case is four levels of severity. There are software tools available that help with this process as well as manage the evidence gathered in support of the remediation process.

> If there is an ongoing oversight of many third parties, simply knowing that the planned reviews are happening is a useful thing to measure.

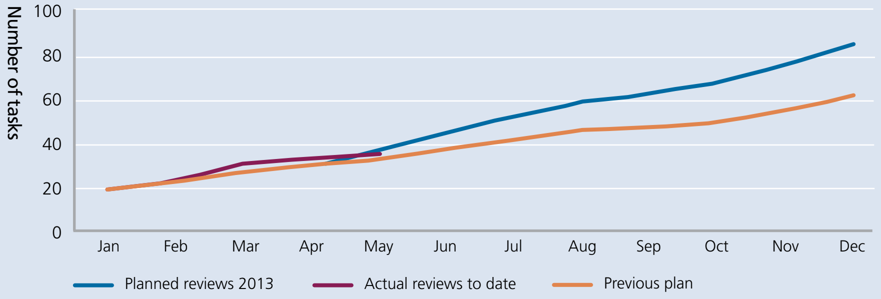


Management oversight of assurance plans

If there is an ongoing oversight of many third parties, simply knowing that the planned reviews are happening is a useful thing to measure. The chart below shows how one organisation has over 90 inspections planned for 2013 which is a re-baseline against the original 65 inspections. The actual plan at May is two inspections behind the plan (net position). However, under the total number of remediation actions we can see there has been a marked improvement from the position at the start of the year with a net decrease of 55 actions. Further good news shows that of the eight inspections in March, there were no parties that required remediation action. The data can be extended to provide detail on the distribution of the severity levels of all the outstanding remediation actions if required.

Such level of transparency enables managers to see both the scale of the task and the progress against plan including any revisions to that plan. There are software tools available that can produce such reports based on the data housed in the system. However, this is a simple spreadsheet solution. Coincidentally, this spreadsheet solution was also used to drive the requirement capture process for the procurement of a vendor management product.

3rd Party Oversight Plan 2013



Progress of 3rd party reviews												
	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
No. of reviews planned	20	4	4	3	7	9	7	7	4	6	8	10
No. of reviews completed	20	4	8	2	2							
Shortfall	0	0	4	3	-2	-11	-18	-25	-29	-35	-43	-53
Remediation planning actions												
No. of parties to remediate	0	4	4	4								
New	173	31	0	12								
Total closed	8	15	37	46								
Total open	165	165	165	110	110	110	110	110	110	110	110	110

> “Rarely does a day go by without a significant software or service provider announcing that their product or service will be migrating to “the cloud”.

Chapter 08:
Cloud: Cyber risk and reality

Chapter 8: Cloud: Cyber risk and reality

Dan Roberts

Abstract

On the one hand the "cloud" provides significant opportunities for business, while on the other, the lack of direct control over cloud-based resources generates concerns over security and performance. In this paper we ask if the "cloud" does result in an increased risk or threat profile. If so, what is the nature of that increased risk, and if not, in what ways is the cloud reducing risks. Our starting point is the concepts of the "Traditional IT Infrastructure" of the corporate IT world, and the world of outsourced services and infrastructure that is the cloud. The overarching conclusion is that the cloud neither increases nor decreases the risk profile; an effectively controlled environment migrated to the cloud will, if the controls remain in place, continue to be effectively controlled, while a poorly controlled environment will be as fraught with risk and threat regardless of the IT Infrastructure choice.

Background

Rarely does a day go by without a significant software or service provider announcing that their product or service will be migrating to "the cloud". Equally, rarely a day goes by in which there in which there is not another report of potential cloud based security weaknesses or threats.

However, an effective information technology (IT) infrastructure is key to most company's ability to perform almost any aspect of their business, thus making threats to IT of critical importance to any business. While most companies are not "IT" companies, failure to provide and manage effective systems can cripple almost any company. Ineffective IT can impact service delivery, slow business processes, impact quality, and limit employee's responsiveness internally and with clients, and undermine the reputation of the company.

What is an "effective" IT environment? It could be argued that a technology environment that enables the company to achieve its objectives for the lowest cost (balanced for risk) is an "effective" environment. IT, while providing core delivery, governance and reporting capability, is viewed and has been viewed as a necessary overhead, and therefore a prime target for controlling of cost, frequently reducing the effectiveness of the internal control environment.

Enter the "cloud". Instead of building, maintaining, and managing the ongoing obsolescence of IT infrastructure, wouldn't it be wonderful to be able to outsource that problem. IT resources are expensive, with the costs of internal infrastructure; people, software, hardware, dedicated server rooms with managed environments, processes and systems of control to ensure protection of critical data, and tested disaster recovery capabilities.

Wouldn't it be nice to outsource all those processes and headaches, while at the same time reducing overall IT costs?

The only "fly in the ointment" is that companies cannot outsource compliance and risk. Cloud may drive down costs, but does it increase total IT and cyber related risk? Outsourcing IT to the cloud carries all the risks that existed before outsourcing, and new sets of risks.

> As with so many trends, cloud has grown to become an all-encompassing term, in this case for the outsourcing of information systems infrastructure in various forms.

Can companies move to the cloud with confidence, knowing that risk is managed, and that data, including confidential and personally identifiable data, is protected? Can companies be confident that levels of service will remain the same or be better? Can companies be confident that capacity will be there when and as required?

While we cannot answer those questions without doubt, it is possible to consider the threats posed by the cloud against traditional IT infrastructure threats. That comparison, depending on each company's risk appetite and tolerance, should provide insight into the real risks associated with cloud in context of the existing risk IT related risk environment that companies currently live with.

Defining "Cloud"

As with so many trends, cloud has grown to become an all-encompassing term, in this case for the outsourcing of information systems infrastructure in various forms. But what is "the cloud", who owns it, where is it, and is it safe? While there are multiple types of cloud (discussed below) conceptually cloud is the migration of capability from within the control of the company to an outsource provider or manager of systems and infrastructure.

Yet even within that definition there are many potential subsets. Are we outsourcing the management of the application, the systems and platforms, or only a subset of the systems and platforms? The potential to migrate any of a range of IT infrastructure into a management environment, while leaving other elements of infrastructure under the direct management of the company itself leads to the idea that there may not be many type of "cloud" implementations.

So instead of talking about "outsourced providers" we now speak generically about something called the cloud. And while we may talk about the cloud, it is important to keep in mind that this in actuality represents one or many different providers of systems and infrastructure to one or more companies or divisions within a company.

The different types of cloud can be thought of along two dimensions – the coverage of systems and infrastructure within the company, and the depth of services provided.

Coverage of Systems and Infrastructure:

Companies need a wide range of systems to operate effectively, from general ledger and financial reporting, logistics, HR systems and others specific to the business of the company. We can think of cloud coverage in terms of the range of systems that are outsourced. This leads to a hybrid cloud environment in which a subset of systems migrate to the cloud, while other systems remain under the operational control and management of individuals within the company.

Depth of systems and services provided:

There are four common "levels" of cloud services(3), which range from providing a complete software and data environment, through to provision of individual servers within a rack of servers in a datacentre. The four levels of service include:

- **SAAS:** Software as a Service, in which the application is hosted and managed by a third party, who is also responsible for the development, maintenance and operation of the software. Examples range from Gmail and Hotmail (now Outlook.com), Salesforce.com, and Dropbox. It is not unreasonable to expect that for almost all business applications, from the most generic to the most specific, there exists a web-based, cloud provided service.
- **PAAS:** Platform as a Service, in which the cloud service provider is used to deliver the total processing capacity required. This includes processors (servers, in any number, logical and physical), disk and backup capacity. In this scenario, the company will load and manage their applications on the processing capacity purchased from the cloud provider.
- **IAAS:** Infrastructure as a Service, in which the cloud provider is responsible for service delivery including operational management of the applications, in effect outsourcing the complete IT department.
- **NAAS:** Network as a Service, in which the company retains control of applications and services, but outsources management of network services including data, telephone and video.

Companies need a wide range of systems to operate effectively, from general ledger and financial reporting, logistics, HR systems and others specific to the business of the company.

Cyber threat perspective

The threat profile of information system goes far beyond cyber threat alone, and while that is a topic of this paper, we also are looking at the range of threats to the IT and information infrastructure. The majority of threats, cyber or otherwise, fall into the following categories:

- **Data theft or loss** covering the potential loss of data for gain of individuals or competitors, damage to the brand, or loss of data resulting in the inability to run the business. Note that the loss of data and the resulting impact on the business is not "cyber" per se, and that the penetration of systems via cyberspace is not the only threat to data.
- **Unauthorised access** to or use of systems and data or information is a threat to any business, and across the business. For example, inadequate management of user rights could result in the creation of fake vendors, unauthorised payments, leaking of corporate plans to competitors, or simply a loss of control over who does have access, and to what information.
- **Private information exposure** can occur through malicious intent (such as from the theft of credit card or banking information, or medical information), or through poorly functioning systems that allow for data leakage. Again, these are threats to the business that may or may not have a "Cyber" component.
- **Availability** for any and all systems is critical for most businesses today to simply "open their doors" to do business. Threats to the availability of systems can originate from malicious external attacks, or simply from poor management practices.

What is important to stress is that threats to IT Infrastructure are not dependent upon an internal or external threat environment, or dependent on "cyber" as the vector for introduction of exploitation of weaknesses. These threats are not new. Our question is: are these threats different in a cloud environment, and if so, is the threat profile greater, the same (but different) or even less than in the traditional corporate owned and managed IT Infrastructure?

The assumptions

The level of reliance that companies place on their access to, and use of, systems has expanded over the past decades to the point where few companies can survive or thrive without their information systems. It has become common to say that "today all companies are IT companies". Of course, this is exaggeration at its best - companies use information systems and IT to deliver their true products and services. Only a small minority are actually IT companies.

Ownership of data

Sometimes it can be difficult to clearly define who "owns" the information. The information produced by or used by the business is owned, but by whom within the business? While we can argue that information produced by the business is the property of that business, there may be limitations on that ownership. Regardless of the ownership of the information, there are levels of protection that are either prudent or mandated, depending on the potential sensitivity of the information.

Personally identifiable information carries a number of legally binding requirements around the protection of that information, while other personal commercial information (such as credit card numbers) is controlled by industry standards. Information internal to a company may have varying levels of sensitivity, and the control of all of that information is at the discretion of the company.

Access to systems

There are two aspects to access to system; physical access and logical access to the data house or processed on systems.

It is common for contracts with software or service providers to contain a "right to audit" clause. These clauses are designed to provide additional comfort to the purchaser of the service, knowing that they can, if required, take a much closer look at the actual controls and activities of their service provider. "Cloud" in these cases is simply another form of service provider, in which there may be the co-mingling of physical infrastructure and data. The right to audit remains an important control, although of varying levels of effectiveness as cloud providers evolve.

We are assuming here that control over logical access to data should be a core concern for companies. As such, the ability to directly manage or verify the setup and functioning of such access controls remains of critical importance.

> Sometimes it can be difficult to clearly define who “owns” the information.

However, regardless of the ownership, the information has value and therefore should be protected. Companies therefore should define the sensitivity (legal or commercial) of information and implement security commensurate with their assessed level of sensitivity.

Ownership of infrastructure

Historically companies have ‘owned’ (even though the equipment may in fact be leased for accounting purposes) their own IT infrastructure, and been responsible for day to day management. This includes asset recording to systems patches and applications, to user access and capacity planning and management. This ownership model has required a significant investment in operational management of the infrastructure. Such management has come at a price, and from an IT Audit perspective, it has been common to see inadequacies in control environments in which effective control would result in increased operational expenditure.

Control over info-security and classification

Closely related to the issue of logical access to data is the establishment of levels of security classification of data. The classification and segmentation of data allows for different levels of security and access. Some information should be available publicly (published price lists, train schedules, etc.) while other information is of a far more confidential nature (blueprints, network diagrams, pricing models, budget, etc.).

Quick history of computing infrastructure

There is a common conception that "cloud" is somehow a new concept, and that with that conceptual world comes a whole new set of risks. Therefore to provide context, we will take a quick wander through the history of IT infrastructure. We begin in the dark past, before the concept of the mainframe, and slide rapidly through history to the present, when the "mainframe" is, in many cases, a variable amount of processing capacity delivered remotely – an "Information Processing utility" just as electricity or water are viewed as utilities.

The dark past

We begin in the dark past, when the concept of a mainframe did not exist, because the computer was the room, not in the room. Grace Hopper (the "Mother of COBOL") told of attempting to identify the reason that the computer stopped. She said "we opened the door and climbed into the computer. There between two relays was a moth, squashed. The moth was removed and taped into the log book, with an arrow pointing to the moth, with the words 'Computer Bug'".

The age of "Big Iron"

Later, we move into the era of Big Iron and the advent of the "mainframe". Monolithic computers with limited networks of terminals connected – a time when a 1200 baud (approx. 4800 bits/second) line was considered an acceptable speed for delivery of data, probably to a physical teletype terminal. CRTs begin to show up, and suddenly there is the ability to directly interrogate the computer and associated data.

1940s ▶ ▶ ▶

Servers

Like all good movie franchises, the Empire Struck Back, and corporate servers began to be introduced, with departmental data residing closer to the department, and corporate data, having flirted with a life on the PC, began its move back to the datacentre.

Thin client

In a foreshadowing of what was to come, vendors developed the idea that there was no need for the personal computer with applications running on each PC – they could run "sessions" on beefed up servers. By doing that, all that was needed as a terminal, not a full PC, with a connection and a browser connected to a corporate "server farm". Security would be re-introduced, and central control re-established.

1980s ▶ ▶ ▶

Mini-computers

From mainframes there is an evolution to the mini-computer, best exemplified by the Dec and the word processing computers produced by Wang. These mini-computers provided the first active peer to peer network environments, in which the monolithic central network was not longer the single source or controller of all data. The move to "End User Computing" had begun.

Personal computer

End User Computing came into its own with the advent of the Personal Computer. By 1985 we begin to see the first portable personal computers – twenty pound metal cases with floppy disk drives, and the earliest hard disk drives. The day of personal data had arrived, and the assumption was that data and processing would continue to push further out from the datacentre, and that one day, corporate IT would be replaced by user developed applications.

▶ ▶ ▶ 1980s

Outsourcing to cloud

It was not a large step to an externally hosted environments in which the corporate servers and systems were transferred to, managed by, and eventually hosted by a service provider. These service providers would outsource the management of IT infrastructure including the systems operations and the entire datacentre and network environments. With control of major datacentres, coupled with the shrinking in size of the physical hardware filling those centres, it became possible to use the same infrastructure to provide computing capacity to additional clients.

Software

Concurrently, software moving through the same evolution, from programs running on giant computers serving a single need, through common infrastructure systems and applications. As applications moved from single user to single corporate, the next step was to multiple users from multiple corporations (large to tiny) accessing a single application environment, logically segmented to protect each company's data.

▶ ▶ ▶ Present/Future

The big break came with the introduction of the personal computer.

History of Control

The history of computing has also been one of the history of control over access to information, ability to manipulate and share data, and the ability to monitor and report on the use of data. The cycle is similar to that of the computers themselves, with control (and flexibility) being limited by the physical constrains of space and the limitations on that processing power of the computers themselves.

The big break came with the introduction of the personal computer. Certainly before then there were distributed systems that were designed specifically either to enable or to restrict access to information. For example, the Multix and Unix operating systems showed very different views on accessing information. Unix was designed to facilitate access to and sharing of information, and the file structures were designed to support this. Multix on the other hand was designed to control access to data. Ultimately, Unix won.

With the PC, not only did access to data decentralise; so did the ability to develop applications to create, manipulate and share information. While there were major benefits to this (think 123 and Excel) there were also downsides, with applications being developed outside of any central control or understanding of what was being done with information. We entered the world of "spreadsheet hell", and some areas of corporate systems remain in that space today.

Servers and "thin clients" (4) provided the ability to deliver some of the power of distributed systems, while also allowing the centre to regain control over data and its use.

The cloud (and existing corporate IT Infrastructure) has completed the circle, allowing central control over access to data and computing, while not completely removing either the benefits or threats of distributed computing. Orphan systems remain core to businesses, and development still takes place outside of the "IT shop". Yet as the same time, SAAS environments are providing the ability for the centre to identify and implement systems that would have been locally developed within the business unit or department.

Going (almost) full circle

So we can see how the hardware and software worlds have gone through an evolution that has brought then almost full circle, from central control to distributed partial control with greater flexibility, back to a world of central controls without total loss of that flexibility. Cloud now provides that almost infinite amount of processing power, under "central" control, while still allowing flexibility in system selection and implementation. The time of custom developed applications to perform common businesses activities is past. Custom application development is now the domain of specialised systems that deliver a significant competitive advantage, while using "COTS" (Commercial off the Shelf) applications for non-unique business applications.

> The cloud (and existing corporate IT Infrastructure) has completed the circle, allowing central control over access to data and computing, while not completely removing either the benefits or threats of distributed computing.

Threats

When determining the threat profile of a traditional IT versus cloud implementation alternative, it is important to consider the specific threats associated with each of the two option. We argue that the range of threats is the same regardless of the selection of traditional IT or cloud. Our list includes:

- Access control
- Segregation of duties
- Information Security
  - Classification and access authorisation
  - External penetration or malware
- BCP/DRP
- Availability
- Operations
  - Backups
  - Load balancing
  - Capacity planning
- Project management
- Ownership
- Monitoring
- Commercial agreements
- Service Level Agreements
- Safe harbour

This enable us to look at a common list of threats and consider them from the traditional IT or cloud perspective. In doing so, we can also consider the mitigation or controls aspects of each, and in so doing, develop a set of questions or tests that we can apply to each option.

The threats: traditional vs. cloud

In considering threats to traditional IT environments, it is worth providing a quick definition. By traditional we mean those IT environments that are hosted within the physical premises of the organisation, be those premises owned or leased, and for which the organisation controls both logical and physical access. Traditional IT environments also include the software, both application and systems/ network, development or managed by the IT department of specialists of the organisation. By “cloud” we mean the range of cloud options defined above.

It is probably worth noting that today there are very few businesses that are completely “traditional IT environments” as almost all exploit to some degree, cloud type services or applications.

Traditional IT Infrastructure	Cloud Infrastructure
Access Control	
Establishment and management of user access is critical for effective management and protection of critical information assets. Processes need to be in place to authorise users, establish online accounts, review accounts and usage, and ensure that accounts are removed once individuals no longer have a business need to access the system or data. This function frequently is assigned to an individual or team within IT, and can be a boring and time consuming activity. As such it is not unusual to find that the processes function adequately at best. Coordination with other parts of the organisation are required, such as HR to confirm new starters, terminations or departures, and changes in role function that require changes in system access.	Migration of systems and data to the cloud or cloud providers does not change the need for effective access control management. Establishment and revocation of access remain non-automated functions based on the matching of individuals' roles and responsibilities, and their need for access to systems. With most cloud based infrastructure, determination and administration of access remains with the service user. Where provision moves to the cloud provider, it is important to put in place review processed to ensure that revocation of access is being performed when requested. **Assessment: No change to risk profile.**
Segregation of duties	
Segregation of duties is a fundamental control, and is applicable across applications and operational functions within IT departments and across the business more generally. The establishment of systems based segregations of duties and the management of those segregations is an important discipline in the traditional IT infrastructure environment. Some examples of segregation of duties include multiple signoffs for payments, isolation of developers from production environments, and not allowing individuals that set up vendors to issue payments to vendors.	Migration to a cloud environment does not alter the fundamental importance of segregation of duties. In addition, it does not change responsibility for implementation and management of system level access, or application level controls and their implementation. **Assessment: No change to risk profile.**

Information security	
Information classification and access authorisation: Access to the right information is critical to effective accomplishment of role responsibilities. This must be balanced the danger of inadvertent or intentional release, theft, or loss of information, depending on the criticality of that information. Information security, through technical access controls, network and application security, and the application of controls over information is critical. To enable this to be accomplished in a meaningful and cost effective manner, the classification of each piece or type of information is needed. Information that is of the highest commercial sensitivity needs to be protected. Likewise, access to client or customer information, in particular personally sensitive or identifiable information, must also be protected. Traditional IT infrastructure has provided frameworks and systems to control access, and to classify information. Separation of servers, disk "farms", encryption and additional monitoring have provided comfort that such information is being protected. Effective levels of information security and protection via segregation, monitoring and security can be expensive and time consuming, and is a classic area starved of resources. The risks can be high, as can remediation costs.	Movement of corporate information to a cloud infrastructure environment does not change the nature of the sensitivity of information. Nor does it alter the threat profile associated with any piece of information. Classification of information remains an important aspect of information security, as is determination of the appropriate logical (and physical) infrastructure. Sharing of critical information on common logical drives in a cloud environment is as dangerous as sharing that information on common drives in a traditional IT environment. **Assessment: No fundamental change to risk profile.**
External penetration or malware:	
A constant threat in IT environments is that of external penetration or the introduction of viruses and other malware. Ensuring that penetration detection and virus/malware scanning systems are current is a constant challenge, and adds an additional cost burden. Further, the proliferation of "day-zero" vulnerabilities and the general delays in identifying such vulnerabilities creates a situation of perpetual heightened threat.	An effective cloud infrastructure should provide a higher level of protection, as the economies of scale available to cloud providers means it is easier for them to implement effective penetration detection, infrastructure based virus and malware systems, and the ability to share the cost burden of such infrastructure across a larger number of clients. From a risk perspective, any migration to a cloud infrastructure should only be considered where the enterprise can have confidence (through contractual assurances and effective referencing of the provider) that such protections are in place. Even with such protections, client-side PCs, laptops and mobile devices will continue to represent a significant threat vector, and the move to a cloud will not mitigate this risk. **Assessment: Some important reductions in risk, while other risks remain.**

Business continuity and disaster recovery	
The provision of disaster recovery capability can be a significant cost to a business. The costs range from equipment and premises, to duplicate software licenses, redundant communications and alternative sites (including operational office space for critical functions). It is an axiom of BCP/DRP that if the plan has not been tested, it will not work. Definition of scenarios and development of test plan, execution of the test and revision of plans can be time consuming and expensive. Failure to do so can render the BCP/DRP investment moot.	In the cloud environment, the primary difference in BCP/DRP is the ability for the cloud provider to provide redundant capacity and communications, with the user company having responsibility for that hardware and software that is resident on company premises, and responsibility for the "last mile" of communications – from the office to the network provider's entry point (which may be the point in the wall, or it may be the local telecommunications exchange). In the cloud environment, the level of recovery becomes a contractual matter, and the primary concerns are around the commercial viability of the vendor. Plans are still needed for non-hosted systems and premises, and plans still need to be tested. **Assessment: The risk profile if different, with some risk transferred while other risks remain.**
Availability	
Uptime availability relies on a number of potential points of failure throughout the infrastructure, from the "terminal" (be it a PC, laptop or mobile device) through local routers, network connections, and "host" systems and the physical infrastructure required to house and maintain each element.	The only significant change in a cloud infrastructure environment is outsourced management of availability of the "host" systems, data and physical support environment. Associated with that change is the ability to include service level and uptime requirements that can be linked to penalties for failure to achieve such availability targets. **Assessment: Potential reduction in the risk profile.**

Operations	
Backups: Backups of data are taken at regular intervals for two primary reasons: to ensure the ability to recreate a situation at a certain historical date/time, and the free online storage, saving space and cost of equipment. Management of backups is a core activity of IT Operations, and backups should always be removed to off-site locations to reduce the risk of a loss of data, and the ability to recover to the most recently saved position. This requires a set of operational disciplines be put in place, including the regular cycling of backups to/from off-site locations, regular recovery tests, and periodic auditing of the off-site registers to confirm that all backup data is accounted for.	Confirmation of backup and recovery capability remains the responsibility of the client, even when the function is performed by or through the cloud infrastructure. Contractual agreements remain only as good as the client's ability to confirm to their own satisfaction that such operational activities are being performed on their behalf. This means that it remains important to periodically perform recovery tests to confirm that backed-up data can be restored as and when required. Equally, the cloud is as fraught with risk as any platform, and the commercial health of any cloud provider should be carefully considered before using such providers for critical functions such as backup and recovery capabilities. For example, on 9 August 2012, The Register (online) reported "Blue Solutions have now received emailed confirmation that Doyenz will no longer be providing or supporting the rcloud backup and recovery service in the UK by the end of this week, 10 August 2012. We understand that Doyenz has emailed UK resellers and MSPs directly to notify them of the change. Doyenz's removal of the rcloud service is surprising and disappointing. We understand that Doyenz will retain client data on its systems until only 31 August 2012. We believe [but this is unconfirmed to us] that Doyenz will offer our UK resellers using the rcloud service the option to back up data to its US cloud servers." **Assessment: The risk profile is not higher or lower, but certainly changes.**
Load balancing: A common refrain heard these days is "throw another server at it" whenever response times begin to degrade, regardless of the underlying reason for such degradation. Processing, memory and storage load balancing has largely become an historical concern, as the costs have continued their "Moore's Law" slide. Yet throwing another server at the problem is only effective if indeed the issue is one of processing speed or capacity. The issue could be memory usage, poorly performing software, ineffective database design, or any of a number of other reasons. There is also the tendency to suggest that each application or user community have its own server, resulting in a proliferation of servers, each running at a negligible utilisation percentage. And with each server, the cost burden for an additional set of software licenses, hardware and "rackspace" increases. At some stage, there is a cost benefit to be achieved through the employment of humans to perform the load balancing – unfortunately it remains difficult to identify when that point has been reached.	The cloud's influence on this issue is directly dependent on the nature of the cloud implementation selected. For example, PAAS (Platform As A Solution) will still result in a need to manage the number of servers and the distribution of applications and databases across those services. IAAS (Infrastructure As A Service) should reduce the risks by outsourcing management of the infrastructure to the cloud provider, and in doing so, outsourcing responsibility for load balancing. Further, in a SAAS (Software As A Service) solution, provision of processing and storage capacity and associated load balancing is fully outsourced. In summary, the PAAS cloud does not provide any mitigation of load balancing responsibility and associated performance and cost risk, while IAAS and SAAS do provide such mitigation. **Assessment: cloud can, depending on the type of cloud, reduce the risk.**

Capacity Planning: Delivery of functionality at response times that meet business needs is the responsibility of a capacity planning programme. The objective has to be to determine approximately when existing capacity will become overstretched, such that additional capacity (processor, memory, storage, and network) can be ordered and installed before performance suffers. It is only too common in the traditional IT infrastructure environment for management to be presented with request from IT for additional capacity outside of the budget cycle. New servers are required, additional memory, etc., or the business will begin to suffer. In one example, a smaller City firm suffered a constant stream of requests of additional capacity, always outside the budget process and cycle. The lack of monitoring and planning meant that the firm was unable to project total IT capital spend.	Dependent on the cloud option implemented, there can be a significant reduction in capacity planning related risk. The city firm mentioned, on moving initially to a PAAS type of cloud, found little benefit, as the platform was provided, yet without the monitoring and projects, unplanned capital expenditure continued to plague the firm. An eventual move to a combined IAAS and SAAS cloud environment, with a per-user fee, and freed the firm from such capacity related cost shocks. They have also gained through reduced headcount (of IT infrastructure support personnel) and as capacity is the responsibility of the IAAS and SAAS provider, they have been able to project total IT costs, and in fact have converted all capital costs to operating expenses that can be projected on a per-headcount basis. **Assessment: Dependent on solution, potentially significant reduction in the risk profile**
Project management	
Change to implemented systems, technologies and processes should be managed through formal Life Cycles and project management professionals. The PMBOK (Project Management Body of Knowledge) provides one commonly accepted set of guidance for delivering projects. In our traditional IT environments, effective project management is fundamental to achievement of cost effective, timely delivery of functionality and process change across the business.	Cloud is the delivery channel for information supporting processes. Project Management therefore should view the cloud simply as an alternative delivery platform. **Assessment: The quality of project management processes and individuals remains the same in the cloud environment.**
Ownership	
Actual balance-sheet ownership of IT resources has been both an accounting and cash flow issue, not a technical issue. Decisions to capitalise certain IT spend (hardware naturally, software, and development activity) has gone hand in hand with the desire to smooth total IT spend, and to control such spend from unexpected changes (as discussing capacity planning above). Fundamentally however, there are few compelling reasons (provided data retention and destruction policies are in place) for a company to actually own (or lease) a particular piece of equipment or software.	Cloud, depending on the type (IAAS, PAAS, SAAS, NAAS) provides the ability to smooth IT expenditure, yet also removes or alters the ability to capitalise IT costs. **Assessment: The risk / reward structure is altered, and FDs wishing to continue to capitalise IT costs may need to consider how this can be accomplished in a cloud environment.**

Commercial agreements	
IT Infrastructure requires a range of commercial agreements, frequently with a large number of providers of materials, consumables and services. Because of the wide range of services, it is important that a vendor database and set of procurement standards are in place and monitored for compliance. A core element of many contracts includes the "Right to Audit". The clauses can be limited in some cases to auditing against the contract itself, while other clauses can be wider, allowing auditing of wider performance issues. Fraud can become 'easier' where the number of suppliers increases, the controls over vendor acceptance are weak, or where there are few people who understand the nature or uniqueness of a service being provided. For example, where maintenance services are required but not fully understood in terms of market costs for such services, it is possible to fraudulently exaggerate the cost of such services, and skimming the extra fees for personal gain (example witnessed by the author, with jail time for the	Commercial agreements do not disappear by moving the cloud, they simply change to reflect the nature and range of services that will be included in a single contract with the cloud service provider. While this can reduce the total number of contractual relationships, it does not abrogate the need to negotiate appropriate contracts, or to ensure that the contracts meet the full range of needs of the user of the service. Further, as cloud providers grow in size and aggregate delivery platforms into consolidated data centres, the Right to Audit, while important, may result in a reduced ability to actually perform an audit of the "datacentre" or other physical infrastructure. Operational support activities could still be audited. **Assessment: Little change to risk profile, no increase in risk.**
Monitoring and service level agreements	
Contracts exist to protect both parties, and as such, monitoring clauses are critical for a successful relationship. We have already discussed monitoring of systems performance for capacity and security reasons. The same focus on monitoring for compliance with contractual obligations (on and by both parties) is equally important. Service level Agreements (SLAs) form a key part of the monitoring process. In traditional IT Infrastructure, it is common for SLAs be represent best endeavours agreements, as it can be argued that there is little point in attempting to impose penalties between two parts of the same business. This cannot be said for third party relationships, and in these, SLAs become of prime importance. Traditional IT Infrastructure environments require SLAs with any external suppliers, for back-up and recovery off-site storage, to delivery of consumable suppliers (paper, toner, scheduled maintenance) and provision of services such as network and power supplies.	The cloud environment does not alter the need for or nature of SLAs, or the need to monitor such contracts and agreements. As such, there is no increased or decreased risk from an SLA or contractual monitoring perspective in moving to a cloud based infrastructure. **Assessment: Little change to risk profile, no increase in risk**.

Our Conclusions

We have discussed both traditional IT Infrastructure environments, and cloud environments. We need to be careful to point out that there is no single profile for the traditional IT Infrastructure, as there is no single profile for a cloud environment. Each has its own peculiarities, as such, the comments and discussion in this document apply as guidance only, and readers should look for similarities to their own environments, and not assume that their IT world is one or the other. It probably is already a blend.

In addition, while a company may be confident that they have control over their IT Infrastructure, knowing which bits are "traditional" in-house managed and which are "in the cloud", it is probably that they do not fully understand their supplier or extended enterprise use of cloud based services. Therefore as the IT strategy is being developed or reviewed, consideration should be given to a review of key vendors or suppliers, to confirm either that their IT environment complies with minimum corporate standards, or to identify potential gaps and required remediation by suppliers to reduce such risks.

Selection

If the decision is made to go to a cloud provider, we recommend that a vendor assessment be performed just as for any significant procurement. This should include vendor background checks, referencing of the service provider, and where possible and appropriate, competitive tendering for services. A detailed needs assessment should be performed and agreed within IT and with the internal user community, to ensure core needs and concerns of all stakeholders are considered.

It's all about the contract

The larger the cloud provider, generally the less negotiating power or leeway exists in the contract. Equally, the larger the purchasing company, the more negotiating power they have. A balance should be sought, to ensure that there is a good match. For critical requirements, confirmation that such requirements will be built into any contract, with appropriate penalties.

Performance targets need to be built into the contract, and Service Level Agreements (SLAs) included as a core element of the contract. The SLAs should cover response times (both at the application level, and at the human to human level), and should include the agreed range of services that will be provided. For example, the SLA should provide for confirmation of disaster recovery / business continuity tests being performed on cloud provider's infrastructure at an agreed frequency. Backup and recovery capability should be included and tested on an ongoing basis to confirm the ability to recover critical data within outage time limits.

It's (also) all about the monitoring

Finally, IT infrastructure, traditional or cloud, must be monitored constantly to ensure that service levels are being met, that potential service issues are being identified early, and to ensure that changes needed are being planned for implementation prior to actualisation of the issue. Of course, the exact date or time of the actualisation of any issue or event can rarely be predicted. What is important is to ensure that both (or all) parties are monitoring such information as is available to ensure that there is as much notice of the event as possible, or to ensure that responses to the event(s) are effective and rapid.

> The larger the cloud provider, generally the less negotiating power or leeway exists in the contract.

References

(1) **(http://www.accountingweb.co.uk/article/sage-moves-mid-market-erp-suite-cloud/543954)**

(2) **(http://www.informationweek.co.uk/security/management/5-dropbox-security-warnings-for-business/240005413** and **http://www.techrepublic.com/blog/security/dropsmack-using-dropbox-to-steal-files-and-deliver-malware/9332)**

(3) **http://www.coso.org/documents/Cloud%20Computing%20Thought%20Paper.pdf**

(4) **http://en.wikipedia.org/wiki/Thin_client** (as accessed on 12/10/2013)

/**
* Checks wether the specified
* create methods correctly.
* (usually in the constructors).
* @throws ObjectCreationException
*/
protected void checkCl
createBean());

“This chapter will examine the business benefits of mobile device use and also look at the threat vectors.”

Chapter 09:
Mobile Devices

Chapter 9: Mobile Devices

Alastair Allison CISM SIRM

Abstract

This chapter will examine the business benefits of mobile device use and also look at the threat vectors. We will examine the key components of a governance model for operating mobile devices within a business environment that considers the importance of identifying critical information assets, how it is protected through the data lifecycle and also the potential for data leakage in the event that organisations adopt a "do nothing" option by using mobile devices fresh from the box. This chapter should be read in conjunction with chapter 8 on cloud risk.

Introduction

Mobile devices are here to stay and why wouldn't they be? Light, affordable and increasingly useful as the app market grows to address user needs for their personal as well as professional lives. It is understandable that individuals and businesses want to adopt such devices for the many cost savings they can bring. In the IRM cyber security survey, over 90% of respondents said their organisations allowed the use of mobile devices for business use.

However, as their adoption grows, online threats are rapidly increasing so there is a growing need for security efforts to match the threat and remain responsive and flexible. But keeping pace with these challenges is fraught with challenges. Analysts suggest that there are 2.5 mobile devices[14] per person. Whereas corporate PC environments have been subject to hardening and protective measures for many years, mobile devices and their comparatively weak security mechanisms are more difficult to manage and control. Of the 90% of respondents to the IRM Survey that said their organisations allowed the use of mobile devices for business use, only 37% of those companies exercised any form of configuration control raising concerns in respect of data privacy and corporate responsibility.

Adding to the concerns of risk managers around the technical control there is also the attitudes of the users. In a Fortinet survey in 2012, one in three respondents said they would contravene business policy banning the use of mobile devices for business purposes. In case we needed reminding, regulators are also issuing guidance to businesses on the use of mobile products and to ensure appropriate technical measures are taken to prevent data losses.

[14] Wikipedia defines Mobile Devices as a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard and weighing less than 2 pounds. It therefore excludes the traditional laptop from the scope of mobile devices.

Mobile devices are here to stay and why wouldn’t they be?

The challenges for any business, therefore, are not just the introduction of the technology but also the right behaviours if critical data assets are to be protected. With the right risk assessment and testing and the right level of staff behaviour, mobile devices can be secured to meet business needs and allow faster adoption of new technologies and working practices.

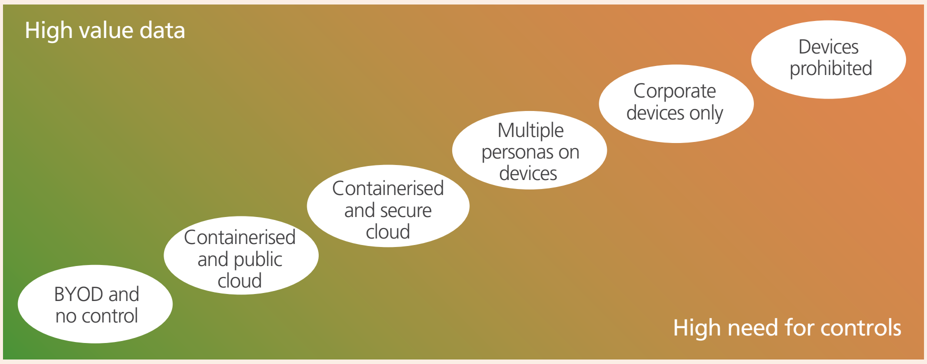
Definitions

BYOD – Bring your own Device: Employee is permitted to bring their own device and use it for work-related purposes

BYODT – Bring your own Device & Technology: BYOD plus the employee’s choice of applications, software and open-source IT tools such as the cloud and software development kits.

The options

There are a range of options available to organisations when considering the use of mobile devices depending upon the value of the data within an organisation and the level of controls that need to be put in place. This is everything from the “do nothing” option where BYOD is permitted with no organisational controls or interference, to the prohibition of devices as they pose unacceptable risk to the organisation. This is represented schematically opposite. Other options may also be available to organisations depending upon their existing or planned infrastructure. For example, using 3G or 4G mobile devices securely connected to the organisational network and using collaborative tools such as Sharepoint rather than having any organisational data on the device.



The relative merits of these options are discussed in Appendix 9.2 to this chapter. However, we do explore the "do nothing" option further within the chapter because it poses some significant challenges if the organisation wishes to reverse that decision at a future point in time. Nevertheless, the idea of this diagram is to show that, with a full and proper risk assessment and clear understanding of the value of the data, a solution that permits the use of mobile devices is probably available.

The risks

The UK Information Commissioner's Office states that mobile devices, particularly under a BYOD policy, "must not introduce vulnerabilities into existing secure environments" (ICO March 2013, p5) and "must not put personal data processes on these devices at risk" (ICO March 2013, p9). However, personal data is not the only type of information that can cause damage to an organisation if there was a loss. Intellectual property or commercially sensitive data such as client lists or the annual results before formal announcement, are all data types that pose a risk to the organisation if lost or stolen. The vulnerabilities of using mobile devices involving the sharing or storing of such data that are highlighted in this chapter break down to five primary risks as follows:

- Malware propagation leading to data leakage, data corruption and physical theft
- Criminal acts including identity theft, fraud or account takeover including unauthorised access to the network
- Accidental or intentional data breach leading to harm to customers, reputational damage and possible fines
- High net worth individuals could be blackmailed or kidnapped
- Interception leading to breach, reputation damage and possible fine

The most likely risk scenario is considered more fully on the following page:

> Notwithstanding the risks, there are many and varied reasons for using mobile devices.

Preconditions	Event(s)	Risk(s)
Personal data is edited on the device. This data may be staff objectives or possibly customer data.	1. Device is lost or stolen or… 2. User becomes a disaffected member of staff or… 3. Family member uploads the data on to their private device from the shared cloud storage or… 4. User uses "Drop box" or similar public solution to bypass controls	There is a risk of data leakage that could affect organisational reputation and could harm individuals or the share price of the Company (see chapter 4 on the 'iceberg' impact).
Sensitive corporate data is edited on the device. The most likely scenario is the use of office-like applications to share innovative designs, amend financial statements, investment options, strategies or M&A activity.		
The user backs-up the device using a cloud solution or another personal machine such as a laptop.		
The user's password for the device or cloud storage is shared with family members or is compromised.		

The benefits

Notwithstanding the risks, there are many and varied reasons for using mobile devices. Those advantages are clearly apparent to the US military who have approved an Android device for operational use and were also evaluating the Apple operating system.

Embracing mobile devices, either as BYOD or corporately provisioned, simply makes sense in the evolution of technology if businesses are to drive down costs, increase innovation and efficiency or even to improve the health and safety of individuals lugging around heavy laptops[15]. They are easy to use and the start-up time is almost instantaneous compared to a laptop.

[15] Laptops weigh between 2 – 5Kgs compared to a tablet weighing a mere 600grams or a smartphone weighing even less at 112 – 185grams.

"mobile services have created new business models that are changing organisational structures and society as a whole."

True, writing reports, designing and completing complex spreadsheets and preparing powerful presentations is not as easy on a mobile device as the applications are not yet there to support the myriad of ways we do business but is there really a need to do these things on the road?

In the realms of business continuity and managing crises, mobile devices are particularly beneficial as they can be used to record notes at the scene, take photographs with location services that tag the photo and get information back to insurers, loss adjustors or medical teams as appropriate. The BCM and crisis response plans can all be stored on the lightweight device and are immediately accessible for use in any location. Those plans that are more sensitive can also be secured but still available via mobile devices. With the wealth of communication methods available from one device, they benefit organisations looking to improve collaboration and responsiveness and all with a single swipe of a finger.

Mobile devices offer a highly efficient tether back to the business. Indeed, ISACA (Vol 1 2013 p13) states that "mobile services have created new business models that are changing organisational structures and society as a whole". Mobile devices offer employees greater freedoms and flexibility. If implemented correctly and with a true assessment of the risks, it can significantly lower IT budgets and management burdens. Mobile devices can also have appropriate segregation of data either by leaving the sensitive data behind or by separating personal and business data. However, realising these benefits is often overshadowed by the significant challenges involved but patience and an implementation strategy will pay off in the end and there are secure solutions for protecting the more sensitive data objects within the organisation.

Key Questions to consider

- Can our infrastructure support it?
- Security implications – what data are we intending to transmit?
- Preventing data leakage?
- When do we have the right to access employee-owned devices?
- Create an internal app store and push specific apps to employee-owned devices?
- Enforcing mobile policy?
- Whitelist and blacklist apps to protect devices and data?
- Physically and legally remotely wipe any device if lost/stolen?
- Who pays for what?
- Employee privacy rights or expectations after they leave?
- Manage compliance or other legal issues?
- Adopt Apple or Android (or both)

The challenge

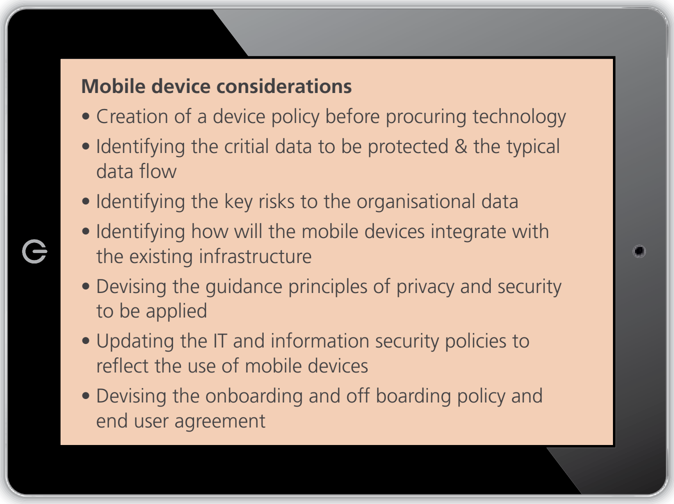
Push back against the use of mobile devices has come from IT Security and the business on the basis of data leakage risks from capabilities such as Apple's Siri and cloud solutions like DropBox. Regulated industries are nervous that they will open a new avenue for data loss breaches that could affect their reputation or regulator censure. However, if organisations are to prevent the underground use of mobile devices, they need to assess the risks to their critical data. A blanket ban on mobile devices is not a viable strategy and above all, it will prevent organisations optimising the opportunities such devices can bring to lower cost, increase innovation and efficiency. Anecdotally, a common response, when asking organisations why they wanted to use mobile devices, was a nod and a wink, "… because the Execs want it". "Business lounge envy" of the latest gadgets, while understandable, is not by itself a robust business case to drive a procurement strategy or to change a business operating model.

Finally, ISACA highlights that "the downside of emerging patterns is the blurring of boundaries between personal and business activity". The "always-on" expectation might increase work pressure and decrease staff morale. This will need to be closely monitored by organisation to prevent burnout and mental stresses and strains. However, if we were to adopt these new technologies and address such concerns, how might we go about implementing a successful mobile device strategy?

The key steps

There are three key steps associated with implementing a successful mobile device strategy. These are:

- Devise the operational framework
- Configuration management
- Data segregation



Mobile device considerations

- Creation of a device policy before procuring technology
- Identifying the critial data to be protected & the typical data flow
- Identifying the key risks to the organisational data
- Identifying how will the mobile devices integrate with the existing infrastructure
- Devising the guidance principles of privacy and security to be applied
- Updating the IT and information security policies to reflect the use of mobile devices
- Devising the onboarding and off boarding policy and end user agreement

Devise the operational framework

How will they be used?

Organisations have to determine how the mobile devices will be used and then decide the extent of the control environment. Understanding what you want to achieve, and why, will help determine the solution. Is it to support marketing staff in front of customers or is it to process sensitive medical data on patients? Does it need to connect to the existing network infrastructure and if so, will that drive the decision on the operating systems and platform types? If security is an issue then it will drive a baseline configuration and tighter asset controls involving encryption standards such as password logons and Transport Layer Security (TLS) encryption instead of the use of a VPN. This is because not all traffic on a mobile device is automatically routed into the VPN tunnel (according to the Information Security experts at ISACA (2012, p40)). There needs to be the assessment and cost-benefit analysis to create an acceptable environment and avoid the creation of a shadow IT infrastructure.

What policies will be applied?

Once the business case is considered, it will be necessary to decide the level of governance to put in place. Who will authorise their use and who will ensure the right configuration is in place? There is also the need to address the necessary policies and procedures such as acceptable use policy, End User Agreement and the Information Security policy that needs to cover the lifecycle of the device including loss scenarios, transfer of ownership, disposal or simply leaving the company. Appendix 9.1 offers an example of an End User Agreement where personal data is not permitted to be shared.

Each of these policies will ensure that staff understand their responsibilities prior to adoption and that the organisation has addressed the risks it is concerned with. Policies also allow reactionary measures to be taken in the event of a breach whereas no policy means there is no hope of a controlled mobile device strategy.

Configuration Management

Configuration Standards

Mobile Device Management (MDM) requires full consideration of the configuration standards and management implications, not only from the perspective of the devices themselves but also from the perspective of the existing network infrastructure. One solution vendor, Aerohive, points out that it is necessary for organisations to "be able to support both agent-based (devices) MDM as well as network-based MDM" to give organisations more control over the risk mitigation strategies and to ensure there is a balance between corporate accountability and personal responsibility. Additionally, there is the need to consider application security controls. ISACA (Vol4, 2013) considers some of the issues for risk managers and IT Managers with regards to network, device or application based MDM:

User support for any restrictive practices on their mobile devices or even on mobile devices belonging to the business is essential.

Network MDM	Device MDM	Application Based MDM
Which devices are permitted on the network	Authorised and unauthorised device inventory	Determine which operating systems & versions are permitted on the network
Determine access levels (i.e. (Guest, limited or full)	Authorised and unauthorised user inventory	Determine which applications are permitted on the network
Define the who, what, where and when of network access	Continual vulnerability assessment and remediation of connected devices	Control enterprise application access on a need to know basis
Which groups of employees are permitted to use the devices	Create mandatory and acceptable endpoint security components to be present on the device	Educate employees about MDM policy

Integration and Support Issues

User support for any restrictive practices on their mobile devices or even on mobile devices belonging to the business is essential. Integration and support need to be considered in the configuration of the devices from the outset to ensure that the MDM solution does not bring the user to the help desk for problem resolution. Enrolment should be simple for users but also allow existing users to enrol in bulk to make the IT task much easier to manage. Instructions need to be clear whilst remaining secure and the MDM solution and configuration needs to be able to quarantine devices that do not meet the approved business policies or breach acceptable endpoint security standards. According to MaaS360, another MDM vendor, all devices "should be configured over-the-air to maximise efficiency for both IT and business users alike" (Maas360, 2012). Risk managers need to consider the implications of this and if it fits with the MDM strategy that has been determined. Nevertheless, if we accept that remote wiping (as discussed later) of devices is an acceptable risk mitigation strategy for lost or stolen devices then over-the-air configuration for the on-boarding process does make sense.

End User Agreements – Make them responsible

There is a joint responsibility for security, data protection and regulatory compliance between the business and users. As a consequence, users need to have their responsibilities outlined in an End User Agreement and even more so if they are likely to have some part to play in configuring the device. Such configuration may be to set the device password capability from a simple 4 digit code to a more complex one that automatically enables encryption of all the data on the device. Users should have access to material and guidance notes on how to configure their devices to remain compliant with the business policies. It is useful if this is done on four levels as shown opposite.

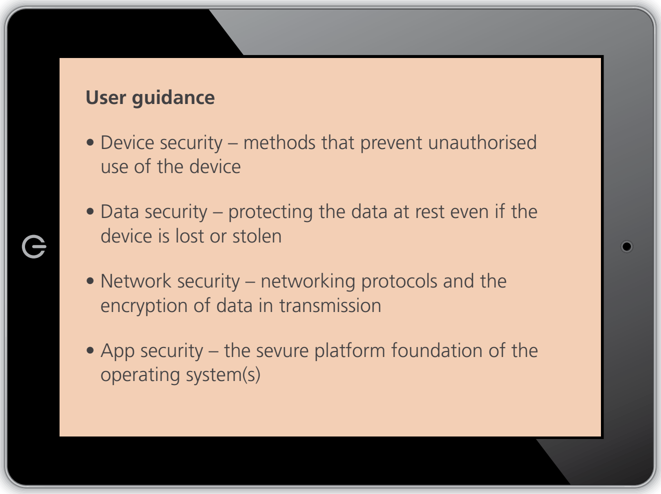
Assistance is available in this area as many of the device providers have the information to hand for organisations. For example, organisations can freely download the Security Overview for Deploying iPhone and iPad for iOSx from the Apple website.

Integration with Cloud Technology

One key area for the risk manager to consider is the acceptable use of the cloud in conjunction with the mobile devices. For example, Apple users can configure their device to allow documents, contacts, emails etc. to be sent to and stored in the iCloud. If a BYOD policy is being adopted as opposed to corporate devices, this poses a significant risk as corporate data and personal data may leak to the cloud. If that device is also used by other family members using a shared iCloud account, there is a risk of accidental data breach if business data is accessed by another family member. For other risk considerations on using the cloud, refer to Chapter 8.

Data Segregation

Identifying the critical data to the organisation and classifying it according to its value will enable organisations to take a tiered approach to its control environment that is proportional to the risk. This extends to how the data may need to be segregated. At the one level, it may be as simple as adopting BYOD and separating the personal and corporate data and not allowing the two to become co-mingled on the device. If data classifications are used, the use of Data Leakage Prevention tools and tools to label emails in a consistent way could prevent certain data classifications from being sent out without being encrypted, thus segregating data types. It is also possible to sandbox applications



User guidance

- Device security – methods that prevent unauthorised use of the device
- Data security – protecting the data at rest even if the device is lost or stolen
- Network security – networking protocols and the encryption of data in transmission
- App security – the sevure platform foundation of the operating system(s)

> There is no doubt that businesses wish to remain competitive as well as attractive to new talent.

so that corporate data is contained in a separate virtual world that can be password protected and encrypted without denying the personal use of the device. Should the device then get lost or stolen, the corporate data can be remotely wiped without compromising the personal data.

The “do nothing” option

In researching this topic we came across organisations that made no attempt to control the use of mobile devices and had not considered the risk. There is no doubt that businesses wish to remain competitive as well as attractive to new talent.

The use of modern technology is a key part of modernisation and in many ways, mobile devices offer organisations opportunities for innovation and value creation but if they wish to capitalise on that opportunity they must do so in a conscious way. Nevertheless, the use of new technology should be accompanied with a risk assessment fully cognisant of the criticality of the data being shared and stored on the device. It may well be that the assessment concludes there is no risk or that the organisation wishes to take the risk but at least that is making an informed decision. The table below highlights two risks that could arise from taking the “do nothing” approach.

Preconditions	Event(s)	Risk(s)
Users do not need to justify their use of mobile devices and the business has no acceptable use strategy or policy.	Users demand custom built applications to support their particular business line or… User shares innovation and creativity with others The company wants to retrospectively apply security policies and controls to mobile devices.	There is a risk that the IT strategy supporting any given line of business is undermined thereby incurring unnecessary or unforeseen costs and challenges to future budget priorities. There is a risk of “data anarchy” existing whereby data is put beyond the control of the company and intellectual property flows out of the company resulting in reputational damage and/or harm to customers.
The use of mobile devices leads to unmonitored creativity and innovation outside of any change management process.		
Extensive user take-up of the mobile device option.		
Inability of the business to manage user expectations and capture and act upon user innovation.		

Risk managers will need to find a balance between what the user wants and what the organisation needs.

Organisations that do not have a sound business case for the adoption of mobile devices will not be able to articulate clearly for what purposes such devices may or may not be used. This is likely to lead to a proliferation of mobile device use and will ultimately increase the risk of data leakage that for some will be incompatible with the regulatory environment within which they operate and for most could undermine the protection of the organisational interests.

Conclusion

Mobile devices are the way ahead for many organisations and offer plenty of opportunities. Risk managers will need to find a balance between what the user wants and what the organisation needs. It will be necessary to protect the secrets that give competitive advantage or data under regulatory protection and look to be less restrictive over the rest. Over-the-air configuration will help organisations achieve operational flexibility within an appropriate control framework but other potential risk issues around ownership and access need to be resolved before implementation begins so that the design can be influenced with the outcome. Nevertheless, the paradigm shift to mobile devices by users is a reality that businesses need to address and those that fail to do so will either miss out on opportunities in the evolving market or face data incidents as employees find ways of using their own devices.

Reading list and websites

Aerohive Networks White Paper, 2012, *"BYOD & Beyond: How to Turn BYOD in to Productivity"*

Information Commissioner's Office (ICO), March 2013, *Bring Your Own Device,*

ISACA, 2012, *Securing Mobile Devices Using COBIT ® 5 for Information Security*

ISACA Journal Vol 1, 2013 – *"BYOD Security considerations of Full Mobility and Third Party Cloud Computing"*

ISACA Journal Vol 4, 2013 – *"Leveraging & Securing the Bring Your Own Device and Technology Approach"*

MaaS360, 2012, *"The 10 Commandments of BYOD"*, accessed via **http://www.maas360.com/products/mobile-device-management in Jan2013**

Appendix 9.1 – Example Mobile Device End User Agreement

The following example of an End User Agreement (EUA) could be used as a template by organisations to ensure that the key risks are addressed and users are fully aware of their responsibilities. This EUA was devised after an organisational risk assessment on the data permitted to be shared in comparison to the data used within the company. It then mirrored its risk adverse culture. Consequently, it is provided only as an illustration and all organisations will need to consider whether its own EUA is fit for the intended use of the mobile devices being employed.

Sample Mobile Device Management Policy and End User Agreement

Reference	xxxxxxxxxxxxxxxxxxxx
Owner	
Enforcement Date	dd-mm-yyyy
Issue Date	dd-mm-yyyy

Purpose

The purpose of this policy is to establish the rules and conditions every user must accept in order to use a privately-owned device for accessing [Company]'s network either locally or remotely, and accessing [Company]'s information by whichever means through these devices. These rules and conditions have been put in place in order to ensure that appropriate protection is given to [Company]'s information which is stored on the private device or accessible through the device. In signing this agreement, the user acknowledges that there is a risk of their personal data being erased by [Company] in the event of a security breach and this data, if not recently backed up, will be permanently lost. Further, the user consents to [Company] implementing the necessary physical controls and technical enhancements to guarantee the protection of [Company]'s information.

In alignment with the [Company] Risk Policy, this policy applies to information in all forms used within [Company], regardless of the format or location in which it is kept

For the purposes of this policy information includes (but is not limited to):

- Correspondence (including e-mail, instant messages)
- Reports
- Documents
- Manuals
- Customer policies
- Electronic or printed information
- Voice (including conversations, phone calls, recordings)

All [Company] employees (including fixed term employees) who are authorised to use a privately-owned device to access [Company]'s network either locally or remotely are required to sign and abide by the End User Agreement.

End User Agreement

1. I have been authorised to use my privately-owned computing or mobile device for conducting [Company] Business.
2. As a user of [Company] Mobile Device Management (MDM) I acknowledge and agree that it is my responsibility to take all reasonable steps to protect [Company]'s information on or accessed through my mobile device in respect of accessing [Company]'s data. Information includes (but is not limited to):
   - Correspondence (including e-mail, instant messages)
   - Reports
   - Documents
   - Manuals
   - Customer policies
   - Electronic or printed information
   - Voice (including conversations, phone calls, recordings)
3. I understand that [Company]'s data may become co-mingled with my private data.
4. [Company] will install an MDM agent on my mobile device to enforce security configuration and to allow remote management. This management will not have access to information other than the configuration on the device. Security Configuration and MDM includes:
   a. Applying and enforcing security settings as a pre-condition of connecting to the [Company] environment and [Company] information
   b. Erasing contents (not limited to [Company]'s information but potentially including private information if absolutely necessary for security reasons) from my device in the event of a security breach or notification from the end-user that the device has been lost/stolen/misplaced
   c. Preventing copies of [Company] information outside the [Company] environment.

5. [Company] will not have direct access to private information on the device. However, in the event of an investigation involving [Company] information the device may be seized, viewed and retained. Private information could also be exposed as part of this. All reasonable precautions will be taken to respect private information on the device, and any investigations will require appropriate authorisation.
6. I will use my mobile device in compliance with the [Company] Policies while conducting [Company] business, in particular the [Company] Risk Policy, and the [Company] Policy for Protection & Privacy of Personal Data, and the [Company] IT Usage Policy.
7. I am responsible for providing, maintaining and paying for my mobile device, cellular service plan for my device, any necessary equipment and accessories for my device, including any additional costs that might occur by using the mobile device.
8. I am responsible for keeping the operating system and MDM Agent application up to date.
9. I am solely responsible for any hardware costs incurred from the loss of my mobile device and any necessary equipment and accessories for my mobile device.
10. [Company] will not provide any technical support for my mobile device and the associated accessories. Technical support will be limited to [Company] software and [Company] applications installed on my device.
11. [Company] may change or terminate this program at any time upon thirty (30) days advance notice. There will be no reimbursement obligation of costs I engaged privately in order to participate in the MDM program.
12. I agree that while using my mobile device I must not edit or save any documents from [Company]'s network that contain any customer data or other personal data.
13. I agree that while using my mobile device I must not edit or save any [Company] data to the cloud.
14. A strong password on the mobile device must be maintained at all times. After 8 failed password attempts to log into the device the device will be automatically wiped.

15. If found to be essential, automatic wipe and MDM Erase will also affect my private information and configuration on the device. I agree that it is my responsibility to make regular back-ups of my private information on the device, so that my private information can be restored to a replacement handset if necessary.
16. [Company] has the right to suspend all information transmission between the mobile device and the [Company] environment and [Company] information or complete a remote wipe in the event that:
    a. the mobile device is not password-enabled
    b. the mobile device has an Operating System that is compromised or that does not meet [Company] IT security standards
    c. a breach of any [Company] Policy is suspected or detected.
    d. I am absent from work for a prolonged period in which case the standard policy for restricting access will apply.
17. I will immediately report any lost, stolen, deposed or transferred privately-owned device under MDM to the IT Helpdesk. If I dispose, sell or transfer ownership of this device, or cease to be entitled to access [Company]'s network, I will remove all [Company] applications and data.
18. I agree to allow [Company] to remotely access my device to remove all [Company] data and [Company] applications should I no longer be authorised as an MDM user.
19. [Company] has the right to audit [Company] data held on the device.

I confirm to have read, understood, and will abide by the [Company] MDM End User Agreement. Breaches of this agreement may be subject to disciplinary action up to and including dismissal.

Date: ______________________________

Users Signature: ______________________________

Name: ______________________________

Appendix 9.2 – Mobile Device Options

Mobile Device Option	Usage	Strengths	Weaknesses
BYOD and no control.	Where there is no risk to personal identifiable information, intellectual property or organisational data.	Staff satisfaction; Could lower organisational costs for IT.	"Data anarchy" could exist; Stable door always open – difficult to rectify data loss risks if the policy needs to be tightened at a later stage; organisational data, templates and client lists etc. easily taken to another organisation; vulnerability through the use of unsecured wifi connections; no user authentication; mobility allows all security controls to be eliminated; unencrypted data storage in storage mediums beyond organisational control; reliant on the integrity of the individual.
Containerised and public cloud.	Where there is no risk to personal identifiable information, intellectual property or organisational data but the company permits email and calendar data to be integrated in a single device as well as viewing of documents and presentations.	Retains organisational data within a virtual box and separate from the personal data; Reduce number of devices a user operates – reduces a small health and safety risk; capability to remotely destroy organisational data in the event of a loss of the device; increase business agility; can aid process efficiency and increase innovation; minimum security baseline and configurations can be monitored and managed remotely; enforced IT policies including user authentication.	Risk of organisational data becoming co-mingled with personal data if email attachments are edited on the device; data leakage of organisational data to the public cloud; data theft if cloud provider is compromised; data put out of reach if not retained on the device; reliant on the integrity and responsibility of the individual.

Containerised and secure Cloud.	A risk to personal identifiable data, intellectual property or sensitive organisational data exists and needs to be mitigated through heightened control environment.	As per above with additional strengths: All valuable data is protected and retained by the organisation separate from the personal data with full remote wipe capability in the event that the device is lost or the individual leaves the organisation.	Increased costs and management overhead compared to earlier options.
Multiple personas on device.	Users only need to carry one device.	Personas are completely isolated from the others; difficult for any malware to infiltrate from one persona to another. Management of personas can be a software as a service and can reduce costs; high satisfaction rate for users who can still play games and use their personal apps without IT policy restrictions.	Integration of calendars and email accounts between work and personal personas may prove difficult; currently limited to Android devices only.
Corporate devices only.	Companies who prefer to control their IT assets, the baseline configuration and the deployed policies.	Consistent configuration management; enforcement of standard security baselines; increased business agility and innovation; data security assurance, retained accountability and responsibility within the organisation.	May not reduce number of user devices held per person; potentially increased costs.
Devices prohibited.	Not applicable.	Absolute security of data with all data being kept within the confines of the established IT infrastructure.	Unlikely to be popular with staff; may lead to unauthorised use or people finding ways around the prohibition; reduces innovation and potentially the business agility.

> “Two thirds of world leaders are engaged in diplomatic relations on Twitter.“

Chapter 10: Social media – managing risks and seizing opportunities

Chapter 10: Social media – managing risks and seizing opportunities

Angeliki Chatzilia

Introduction

"The message is the medium".

Using those words, Arthur McLuhan expressed in 1964 the idea that people tend to focus on the obvious. What McLuhan meant is that, by this focus, people largely miss the structural changes in our affairs that are introduced subtly, or over long periods of time. Whenever we create a new innovation – be it an invention or a new idea – many of its properties are fairly obvious to us. We generally know what it will nominally do, or at least what it is intended to do, and what it might replace. We often know what its advantages and disadvantages might be. But it is also often the case that, after a long period of time and experience with the new innovation, we look backward and realize that there were some effects of which we were entirely unaware at the outset[1].

What happens then when the medium is social? What are the anticipated effects it has on its users? And how does it turn into a Cyber Threat that can harm your organisation? This chapter is targeted at presenting the cyber risks and opportunities associated with the use of social media in organisations as well as the strategy and tactics that stem from best practice regarding their management.

A ubiquitous phenomenon of unprecedented impact

Two thirds of world leaders are engaged in diplomatic relations on Twitter. In 2012, the **Fortune Global 100 Companies were mentioned more than 10 million times online in one month, with most user chatter happening on Twitter.** 87 per cent of those companies are using at least one of the major social platforms to communicate with stakeholders online. As of January 2013, Facebook has more than 1.15 billion active users[2].

Although these figures demonstrate the impact and the extent of the use of social media nowadays, the vast change that they have brought to our personal, social, political and business lives has become obvious to every individual who lives in modern society.

The power of social media is such that it can be used to instigate and co-ordinate political revolutions and bring down Governments. It is not too difficult to understand what damage it could do to businesses. By shifting the power from the organisation to the individual, their use has shaped a new set of rules to the market arena arguably shaping the entire global social construct. Social and economic actors, from large multinational organisations to power exercising individuals and senior management, coexist and are part of an interactive ecosystem consisting, inter alia, of social media users and their output. Effective control over typical media channels has undergone a paradigm shift away from organisations to the ordinary person.

> The power of social media is such that it can be used to instigate and co-ordinate political revolutions and bring down Governments.

The aforementioned characteristics render social media both a valuable tool and a catastrophic threat to the ones that are affected by their use in various different ways.

On one hand, social media is considered increasingly a vehicle for organisations to interact with internal and external stakeholders: organisations are using social media tools and 'big data' platforms to build brands and communities which can engage customers in regular feedback dialogues; HR managers look for job candidates on LinkedIn and XING; R&D teams publish their development guides on corporate Wikis; and technical support personnel use instant messengers to discuss in real time critical issues with the product.

On the other hand, the extensive use of social media renders organisations subject to numerous risks that can cause serious damage to them if not managed properly. The fact that in the UK more than 51 per cent of organisations do not address social media risk as part of their risk assessment process, with 45 percent indicating that they have no plans to do so in the coming year's audit plan, reveals the perfunctory management that those risks receive. Additionally, of those that do address social media risk, 84 per cent rated their organisation's social media risk-assessment capability as "not effective" or just "moderately effective."

Due to the aforementioned reasons, social media has to be taken seriously into account by senior management, audit committees and boards of directors. These actors must ensure that they not only identify the risks and opportunities that social media engenders but also have the right risk management mechanisms in place in order to manage them as effectively as possible.

Finally, this chapter does not seek to provide an unequivocal definition or a list of what social media is and includes. As a rapidly evolving reality and uncharted territory, rather than a static list of platforms, social media is not a term that could (or should) be strictly defined. However, in the context of this chapter, social media can be seen as the means of technology-supported and internet-based interactions through which users can create, share and/or exchange information and ideas for numerous and diverse purposes, such as entertainment, business, communication, recovery after disasters and education.

More than 50 percent of social media users post personal information that exposes them at the risk of being attacked or harmed, or, in other words, at the risk of Social Engineering Attacks.

Risks

Several different types of categorisation have been proposed to classify the risks associated with the use of social media in the organisational context. However, the selection of one of them does not affect the identification of risks. According to the following classification, some events and conditions interact with each other and generate causal relationships. Therefore, a risk may be triggered by more than one event and thus pertain to more than one categories.

Social media risks are associated with the people involved in the organisation as well as with the information and the technology the organisation utilises so as to perform its operations and meet its objectives. In line with this, social media risks can be classified under the three following categories:

1. Risks that are associated with people;
2. Risks that are associated with technology; and
3. Risks that are associated with information

1. Risks associated with people

- ***Social Engineering Attacks:*** A study by Consumer Reports revealed that more than 50 per cent of social media users post personal information that exposes them at the risk of being attacked or harmed, or, in other words, at the risk of Social Engineering Attacks[3]. These attacks occur when posted information, which can be confidential, sensitive or useful in other ways, is used by a third party who subsequently uses it for malicious purposes. The information can refer either to the individual or to the organisation the individual works for and the attacker can exploit it in various ways. For example, such an attack might be used to gain access to an organisation's assets by coercing an employee or consumer to provide user IDs and passwords or by coercing the individual to execute a virus or Trojan.

- ***Account/identity hi-jacking and weak authentication:*** It is common practice for organisations to use challenge questions in order to validate the identity of people who are using the corporate or personal social media pages or other corporate IT systems. However, many times the answers to these questions can be found on the individual's own social media page or profile. Indeed, a Microsoft-Carnegie Mellon study reveals that 28 per cent of the people who are known and trusted by the study's participants could guess the correct answers to the participants' challenge questions. However, even people not trusted by the participants had a 17 per cent chance of guessing the correct answer to a secret question after accessing their social media profile[4]. As it becomes evident, the fairly basic methods and simple password controls that social networking sites use in order to verify a users' identity render quite easy the creation of a 'fake' organisational account; or give the ability to an individual to pretend to be another individual; or to take control of an organisation's page in social media. This tactic is commonly known as account or identity hi-jacking and its consequences can be severe for the subject of the hi-jacking.

Last February, Burger King faced a relevant social media problem. The company's Twitter account had been hacked — its name had been changed to McDonalds and its background replaced with an image of Fish McBites. In the hour it took for officials to regain control, hackers proceeded to send 53 tweets to the burger chain's more than 80,000 followers, ranging from the mildly funny ("if I catch you at a Wendy's, we're fightin!") to the patently offensive ("We caught one of our employees in the bathroom doing this...," with an image of a drug user shooting up)[5].

- ***Oversharing and Exposure of Unprofessional Employee Behaviour:*** One of the most revealing examples of this risk is the case of Domino's Pizza. The company had a shocking experience in April 2009, when two employees posted on YouTube a video that showed them contaminating sandwiches and pizza with body fluid. The video was spread through YouTube and other social media all over the Internet, bringing very quickly the company in front of a significant public relations problem. As Domino's spokesman Tim McIntyre noted, "Even people who've been with us as loyal customers for 10, 15, 20 years are second-guessing their relationship with Domino's, and that's not fair."[6]

Apart from that example, oversharing of corporate information by employees can also happen unwittingly. It is true that a large number of social media users post information about their work. A recent study of Twitter users found that 62 per cent of them tweet about their work, with more than one in 10 doing it daily[7]. Additional leakages can come from contractors, vendors, partners, and affiliates. As it will be explained further below, such behaviours can expose the organisation to data breaches and loss of confidential information, the implications of which that can be staggering for the organisation.

- Candidate screening: social media sites are increasingly used by employers in order to check candidates' profiles for additional information. Nevertheless, by checking these sites the employer may end up yielding information that, although being publicly available, the candidate has not volunteered to share with the company. As a result, there is a possibility that the disclosure of a candidate's race, religion, gender, age or sexual orientation can wrongly exclude him or her from getting hired at a position they are absolutely qualified to cover in all respects.

  From a different perspective, there is also the risk that the information provided online do not reflect the actual qualifications that the candidate has obtained. Inflated qualifications or a doctored photograph could lead employers to make incorrect assumptions and recruit the wrong people.
- ***Decisions on Dismissals:*** The few cases of dismissals that have occurred in the UK due to inappropriate use of social media by employees indicate that whether a dismissal is considered fair or unfair at a legal level depends mostly on the context within and the conditions under which it occurs. Recent Acas (Advisory, Conciliation and Arbitration Service) guidance indicates that social media misconduct should be dealt with in the same way as "normal" misconduct[8]. Clearly, then, a determining factor is the employer's implementation of a social media policy and how the employee's behaviour fares against this. Hence, as with all dismissal decisions, any that involve information from social media sites should be reviewed carefully by the HR and legal departments of the company. In particular, companies need to consider both their HR policies and their social media policies in light of the possibility that any dismissal or workplace dispute may become public very fast. In the absence of clear and well-articulated social media policies, the company would face the risk of facing legal consequences, payment of fines or public discontent.

  There are several stories that prove how employee dismissals can go dramatically awry in the era of social media. For example, Applebee's waitress Chelsea Welch was fired for posting a photo on Reddit that showed a customer receipt inscribed with an anti-tipping message from a pastor: "I give God 10%. Why do you get 18?" Between the original Reddit post, Welch's subsequent article for the Guardian and a flurry of on- and offline coverage, Applebee's found itself at the centre of a firestorm that gave everyone, from labour organisers to social media evangelists something to agitate for and feel annoyed with[9].

> There are several stories that prove how employee dismissals can go dramatically awry in the era of social media.

- ***Productivity and Professional Standards:*** According to a study conducted by uSamp in March 2011, social media is listed as one of the causes for approximately 60 per cent of work interruptions[10]. Such statistics increase even more organisations' concerns regarding the impact of social media on their employees' productivity and nurture the impression that social media captures their attention and leads to the waste of valuable time. Undoubtedly, loss of productivity will occur if social media is mismanaged by the organisation and its people.

  Also, inadequate use can undermine professional standards, because social networking at work can blur the lines between personal and professional life. Finally, there is also the possibility that as employees connect with one another on social media hostile work relationships may be created. This can happen if some employees get offended by information they find on their colleagues' profiles.

  In order to deal with those issues, some organisations decide to establish policies that prohibit employees from using social networking sites and block their access to them from corporate devices. However, the effectiveness of such measures is questionable at best. First of all, it is probable that employees will still be accessing social media sites from their own devices. Most importantly though, such measures can harm the company, because employees will not be able to utilise social media to reach customers and seize a wide range of other opportunities.

- Physical Safety: Online activity can lead to actual physical attacks if users of social media reveal personal details such as their address, family details or location (either directly or indirectly). The likelihood of this risk materialising increases when it comes to people that have significant roles or key positions in society, politics and the business world.
- Governance: The option of personal and direct internal communication that social media provides to the employees of a company can undermine the norms and lines of authority that exist among different levels of the hierarchy and, thus, affect negatively the effectiveness of the organisational structure and the quality of administration. Of course, such a risk is more likely to occur when social media is used by a critical mass of employees that communicate through it with each other.

One of the major risks that organisations face as pertains to social media is the fact that they cannot control what is posted about them online.

2. Risks associated with Technology

- ***Malware and viruses, flash vulnerabilities, and XML injections:*** One of the most common ways in which hackers gain access to passwords and sensitive data, as described above, is through malicious links posted on social media sites. Therefore, uncontrolled browsing and access to social media web sites and applications provide the opportunity to would-be attackers to direct malicious content to an individual user or lead him to downloading malicious content from a compromised or malicious website. After all, according to a survey performed by the Ponemon Institute, computers that are used to access social media websites face a greater risk of being hit by a virus or other malware[11].
- ***Audit control:*** The content of the data transfers that are made through social media cannot be easily audited. Moreover, organisations ignore the motives and intentions of social media users who store information that refers to their brands. This inability to monitor or record communications can also disable organisations to enforce copyright controls if they need to.
- ***Content Control:*** One of the major risks that organisations face as pertains to social media is the fact that they cannot control what is posted about them online. Indeed, social media outlets typically involve frequent and far-reaching exchanges with consumers and customers. Hence, a simple message or consumer complaint handled poorly will be seen by many people. Failing to control the accuracy and integrity of such exchanges or even limiting the interaction by taking a post offline, could quickly damage an institution's reputation and brand.

  In addition, unfavourable changes to products and services may also return to haunt institutions through social media. For instance, a prominent bank that announced plans to charge new fees for using debit cards was forced to withdraw those plans in the midst of a flurry of consumer criticism, much of which was escalated through social media.
- ***Continuity:*** As social media is used more and more by suppliers and vendors to collaborate and coordinate with each other as well as by companies to reach their customers, the consequences of an attack against the social networking sites that an organisation utilises to perform its operations become discernible. More specifically, the continuity of the organisation will be radically affected if these sites are rendered unavailable and, thus, service will be lost.

- ***Technical fault:*** The vulnerability of some social media sites to technical faults can result in a failure to implement the user's privacy settings. In this case, information that is confidential, personal or sensitive in other ways may be released.
- ***Bandwidth:*** Ponemon Institute recently surveyed over 4,000 IT security leaders in 12 countries and, according to their answers, one of the top two negative consequences of widespread social media use is reduced IT bandwidth (77 percent) – a fact which increases costs. In the context of an organisation, if there is lack of proactive management and adequate planning, insufficient bandwidth will cause problems to all the services that rely on the bandwidth[12].

3. Risks associated with information

- ***Reputation:*** Perhaps the most damaging potential impact of social media is the one it can have on the reputation of an organisation or an individual. Employees, customers, suppliers and vendors not only can be an organisation's greatest ambassadors, but also can undermine its brand and public image. At the same time, social media users can post defamatory comments about a business and its products – or services – and then share it with each other. After all, no one can control or change what is posted online.
- ***Legal and regulatory risks:*** The fact that content is posted, accessed or distributed by users or employees through the organisation's social media pages renders the organisation subject to certain obligations regarding compliance with regulation and certain legal frameworks. Failure to comply with such schemes can create financial and legal liabilities to the organisation. Exposures to legal liability can derive from, inter alia: slanderous, libellous, or defamatory comments; leakage of sensitive information; online bullying; and breach of intellectual property rights.

- ***Crisis Management:*** Cases such as that of the Arab Spring have demonstrated how extremely powerful social media can be in serving as a vehicle through which pressure groups form and gain voice. In a crisis situation, virtual pressure groups can be created so fast that the organisation will be unable to respond promptly, whereas an inappropriate management can aggravate both the crisis and its consequences.
- ***Data Leakage:*** In the era of big data, organisations receive, produce, edit, share and store a massive amount of information on a daily basis. According to the 2013 Information Security Breaches Survey in the UK, 14% of large organisations had a security or data breach in the last year relating to social networking sites[13]. From confidential documents and internal communication to trade secrets and intellectual property, data can be leaked and even become publicly available via social media websites. Once this happens, it will not be possible to fix the damage by completely deleting what has already been posted online. Data breaches take place when employees accidentally or deliberately send valuable corporate data to destinations outside of the organisation's network borders.

From many perspectives, the consequences for the organisation can be disastrous. If the company's competitive advantage is based on the information leaked, a data breach could damage irreversibly the company's strategy and, as a consequence, its financial performance. Moreover, a disclosure of client information can lead to loss of trust and confidence towards the organisation from the clients' side or cancellation of cooperation between the two parties. Finally, other potential implications of inadvertent information leakage are the detriment of its reputation or the failure of the organisation to comply with information security laws and regulations.

HMV, the international media retailer, has experienced a relevant traumatic data breach incident in the past. In January 2013, a disgruntled social media manager hijacked one of the company's social media accounts and made available to the public details about recent layoffs and mismanagement[14].

> Companies need to have policies that set guidelines regarding what acceptable use of social media means to them and their employees.

Responses to Risks

None of the myriad risks associated with social media use can be eliminated completely. However, taking a thoughtful approach and structured approach to understanding and assessing the risks and then developing and implementing a comprehensive plan will reduce significantly an organisation's susceptibility.

1. ***Development of a social media policy:*** Companies need to have policies that set guidelines regarding what acceptable use of social media means to them and their employees. These policies should address areas such as employee use of social media at work, social media use during employee hiring or termination, and vendor management policies. In addition, policies must include all the types of sites and channels that the term 'social media' refers to, such as YouTube, Pinterest, Google+ and micro-blogging sites, instead of focusing only on the most obvious media, such as Facebook and Twitter.

2. ***Engage a multidisciplinary team:*** Many organisations mistakenly think of social media as an IT or marketing problem. Because social media activity can affect a wide range of departments and functions, representatives from all the affected groups must participate in order to address the issues related to social media. An effective strategy brings together senior members of human resources, legal, IT, marketing, risk management, public relations, compliance, audit, and any other affected function. The team should be formally chartered so that each person understands his or her role and responsibilities. A project or programme manager should help the team track and maintain progress.

3. ***Training:*** All levels of hierarchy must receive proper and regular training on how to implement, monitor and enforce the guidelines that the policy has set out. However, top management, brand managers and social media page administrators have to receive tailored training, as they have key roles as ambassadors of the organisations at an external level and as leaders that define the tone-from-the-top at an internal level. The content of the training sessions must include security and compliance issues, as well as more advanced themes, such as using social media for sales and improvement of internal workflows. In addition to this training, companies can also take advantage of the online courses and webinars for users that some of the best social media tools now come equipped with.

4. ***Careful handling of customer complaints:*** social media pages nowadays have in many cases replaced the conventional customer service helplines. At the same time, the amount of feedback, reviews and complaints that companies' see posted about their brands and products on social media is massive and happens on a daily basis. Because of the fact that both this information and the companies' responses take place in front of the "eyes" of other social media users, careful handling is more than necessary. Some companies have made situations worse by simply deleting negative posts or tweets. Others have engaged in online arguments with users on social networks, unwittingly creating bad publicity. The better strategy though is to have a measured response, informing the user about what is being done to address his or her concerns. If the issue is particularly complicated, the dialogue must continue to a one-to-one basis, either on the phone or via email/message.

5. ***Review the terms of use of social media sites:*** Another important factor that has to be taken into account is whether the organisation understands and follows the terms and conditions of the social media it uses. This is particularly important when running promotions and competitions, as in some of these sites, not complying with their rules can mean that your page risks being removed.

6. ***Monitoring of the company's own pages:*** A company's social media mitigation strategy would be incomplete without the company actively monitoring potential social media activities that may expose it to risks. More specifically, attention must be paid both to the content generated by followers and friends of the company's social media accounts and to that posted by employees. In these terms, the company's policy must be clear about who is allowed to publish messages on behalf of the company. The organisation can also keep track of social media issues related to it by using social customer relationship management (CRM) tools.

7. ***Keep access as low as possible:*** Ensure you are using a positive information security model logically and administer privileges with a 'least-access-necessary' mindset. Less people with access to sensitive data both from a network perspective and a logical access perspective significantly reduces your risk in losing data through a social engineering attack.

8. ***Avoid the use of simple passwords:*** The most common password in 2012 was still "password"[15]. Sometimes, an effective password is the only barrier standing between an individual or organisation and a cyber-attack. Therefore, it is important that both the corporate and the personal accounts of an organisation and its employees are safeguarded through strong passwords. In addition, as highlighted above, it is essential that the people who know the company's passwords are limited to a necessary number and known by the company.

The most common password in 2012 was still "password".

Opportunities

The advantages of social media when used in the right way are multiple:

- ***Communication with a massive audience and a global market:*** According to a recent study by Burson – Marsteller, 80 per cent of social media users prefer to connect with brands through Facebook[16]. This fact gives an idea of the potential that businesses can unlock if they utilise social media effectively in order to advertise and promote their brands. More specifically, social media can serve as a vehicle for them to reach a massive global audience in a direct, interactive and – usually – free way.
- ***Continuous improvement and Innovation:*** The feedback and criticism that a business receives through these channels nurtures and orientates efforts towards progress and continuous improvement. In this way, the business understands its customers' needs, attitudes and experiences and provides new or improved products and services accordingly.

  When Gap used Facebook to announce their plans for a new logo a few years ago, it was hit with a massive amount of negative comments. However, Gap managed to turn the situation around and make the most out of it. More specifically, not only did the company listen to the negative comments regarding their new logo, but it also did something essential about it. After trying to alleviate the situation by giving fans the opportunity to submit their ideas for a better logo, Gap decided to revert back to the logo they had had for more than forty years. In this way, Gap established a new sense of trust with their community, which feels as though it is now part of the logo and the brand. In addition, by introducing the new logo online before it went out, Gap saved the high expenses associated with rebranding their stores and advertising.
- ***Digital Word-of-Mouth:*** When existing customers share positive comments or experiences regarding products or services, they can inspire the confidence of new customers and be an important deciding factor for choosing a company over its competitors.
- ***Enhanced relationship with clients and consumers:*** The information gathered through social media enhances businesses' market intelligence and enables them to understand profoundly their relationship with consumers, while the digital intelligence acquired informs the marketing, sales and media relations activities. Retailers, for instance, are collecting data from multiple social media sources in an effort to offer their consumers products that meet more closely their personal goals, such as a healthier lifestyle. Furthermore, insurance companies are combining customer information gathered through social media with real driving data collected from car censors so as to tailor their policies and premiums in ways that reflect real risk and are not based only on the criteria of age, gender and geography.

- ***Talent:*** Acceptance of social media in the workplace could serve as a criterion for talented candidates to pick a specific organisation for employment instead of other employers who are not embracing this access. At the same time, human resources departments take advantage of social media as a tool for recruiting new talent.
- ***Crisis management:*** social media can be used by governments, organisations, mainstream media, and the public to make the flow of information instant (and instantly helpful) when help is needed most. For example, one Facebook user created a Hurricane Sandy news page that received 191,000 likes and that dispensed loads of information critical for those wanting to know which areas were safe, to identify the where their friends and family are, and to stay aware of the progress of relief efforts.

  In the case of organisations, social media can help them prevent a flow of false, misleading or negative information by replying timely and effectively to certain events and crises. "If someone searches your brand, you want them to see the following results page: your paid ad, your corporate website, your blog, Facebook page, YouTube channel, LinkedIn, your tweets and Twitter account, says Lindsay Durfee of PR/PR. "Because now you have taken up almost all 10 spots on the search results pages of Google, Yahoo! and Bing. Customers searching for you will see everything you have to offer instead of websites trashing your organisation."

  Besides, the more active a company is in social media, the more "friends" and "fans" it will have. As Erik Deckers, author of the books Branding Yourself and No Bullshit Social Media, notes, "these people may be able to help a company through a crisis. Instead of relying only on internal staff to help mitigate the damage, the company will have a group of consumers that may do some work for them."
- ***Coordination in the context of the extended enterprise:*** Initiators and intrapreneurs are not just using social media to make their efforts more transparent and accessible; they are using these platforms to improvise and organise new ways to get the job done. They are using these tools and technologies to add value to existing processes or to create new "just-in-time" processes (and programmes) that the C-suite and other senior managers had never envisioned. Social Media inside and out of the enterprise lowers the costs and increases the power of individuals to productively coalesce and coordinate on their own initiative.

  For example, implementing a multi-media proposal developed by MIT students, a company's supply chain and procurement teams utilized LinkedIn, private Tweets and cut-and-paste Sharepoints to quickly coordinate go-to-market product changes with key vendors. By overcoming diverse issues, such as incompatibility among communications networks and the lack of a proactive IT department, the ad hoc network enabled suppliers to transparently coordinate and collaborate with each other as well as respond to their customers' requests.

> Before, while and after an organisation builds its social media strategy, it is essential that it listens to what is being said on social media.

How to seize opportunities

As every industry, brand and organisation is characterised by specific needs and attributes, best practices regarding social media cannot be generalised. Rather than being a panacea to heal the gaps and possible mistakes that companies' conduct in the context of their marketing and corporate strategy, social media should be seen as a tool that facilitates the communication of an organisation with its stakeholders and empowers it to seize the wide range of opportunities that the digital era has to offer. In order to achieve that though, there are several parameters that organisations should have in mind. These are the following ones:

1. ***Listening is essential:*** Before, while and after an organisation builds its social media strategy, it is essential that it listens to what is being said on social media. Listening must not be limited to the competitors and the target audience of an organisation, but it should rather include all the wider conversations that take place on social platforms.

2. ***Analyse what you "hear":*** By listening to its current or potential audience, the organisation collects for free data that can be distributed to utilised by its various divisions: from sales and marketing to production and finance. In addition, it enhances its database in a way that renders much easier the conduction of benchmarking analysis as well as the comprehension of what the current trends and the main influencers are.

3. ***Build the right strategy for your organisation:*** As Kelda Wallis of Tempero Social Media Management highlights, "the key in determining your social media strategy is to understand your social purpose. In other words, find what you can give to your audience and how you want to connect with it". In doing so, the organisation has to create strategy that is based on the value it can deliver to its customers and fully considers the appropriate use of social media channels in order to match its unique attributes. Finally, the social media strategy must not be isolated from the corporate one. On the contrary, is should embrace and support all the components and functions of the organisations in the best possible way.

4. ***Communicate your social media strategy adequately:*** All levels and employees of the organisation must be aware of how social media are utilised by the organisation. However, it is equally important that they are communicated what they are allowed and not allowed to post about the brand, the works place or their colleagues online. Also, it is essential that top management gives the right tone-from-the-top by embracing the social media strategy and policy and by being the ambassadors of the brand on the different platforms.

Content posted and the manner in which the organisation uses social media must be monitored systematically in order to assure that they are aligned with the corporate strategy and objectives.

5. ***Governance:*** Each division must know how it can utilise social media in order to take full advantage of it, but it must also understand that only the social media team gives permission for content to be uploaded online and to coordinate social media-related actions.
6. ***Monitoring:*** Both the content posted and the manner in which the organisation uses social media must be monitored systematically in order to assure that they are aligned with the corporate strategy and objectives. In this way, if any deviations are observed or an unexpected event takes place, the organisation will be in a position to take action timely and effectively.

Conclusions

To sum up, social media can be a double-edged sword for organisations. On one hand, social media can be a very a valuable business weapon, as it allows the organisation to communicate in a personal, direct and costless way with its stakeholders as well as to utilize a wide variety of multimedia to reach its audience. In the virtual world that social media delineate, space is not a limit either. A brand can become present in markets it had never imagined of, whereas data can be analysed so as to meet the needs and characteristics of new clients. Finally, the, company can deploy social networks to administrate and organise itself in a more cohesive and direct manner and hence perform its operations in a timely and efficient manner.

On the other hand, social media is still an unchartered and constantly evolving environment that can sometimes be difficult to use safely and productively. Risk managers and senior management have to ensure that the proper measures are in place to guard corporate data, secure connections and protect against increasingly common malicious attacks that take place via social media.

According to the analysis realised in this paper, the answer to the cyber threats the organisations are exposed to due to the use of social media is not to ignore social platforms or ban their use within the organisational premises. Organisations must rather realise the uniqueness of the advantages that this tool can offer them and make sure that they allocate the right resources through an adequate strategy so as to turn social media into a vehicle through which they deliver value to their audience.

Questions for Executives

Are you using social media in your organisation (Facebook, Twitter, LinkedIn, etc…)?

If the answer is no, think about it again before you reply and reflect on the next question.

How do you track what your employees, your customers and the public say about your organisation on social media?

How do the various departments/divisions in your organisation use social media in the context of increasing sales, supporting operations and internal communication?

Have you developed a social media strategy? If yes, how do you verify your employees understanding of it?

Have you trained your employees so as to increase their awareness of risks and opportunities associated with social media use?

What is the structure of roles and responsibilities regarding social media in the context of your organisation?

How has your organisation made sure that it is able to manage a crisis related to a social media incident (e.g. an employee dismissal gone public via Twitter)?

Bibliography

[1] McLuhan, Marshall. Understanding Media: The Extensions of Man. New York: McGraw Hill, 1964.Federman, M. (2004, July 23). What is the Meaning of the Medium is the Message? Retrieved 09-08-2013 from

http://individual.utoronto.ca/markfederman/article_mediumisthemessage.htm

[2] Burson – Marsteller Twiplomacy Study 2013: **http://twiplomacy.com/twiplomacy-study-2013/**

[3] **http://www.consumerreports.org/cro/news/2010/05/consumer-reports-survey-social-network-users-post-risky-information/index.htm**

[4] Robert Lemos, "Are Your 'Secret Questions' Too Easily Answered?," Technology Review, May 18, 2009, **http://www.technologyreview.com/web/22662/?a=f**

[5] **http://www.bbc.co.uk/news/world-us-canada-21500175**

[6] **http://www.nytimes.com/2009/04/16/business/media/16dominos.html?_r=0**

[7] Chloe Albanesius, "8 Percent of American Web Users on Twitter, Pew Says," PCMag.com, Dec. 9, 2010,

http://www.pcmag.com/article2/0,2817,2374100,00.asp#

[8] **http://www.acas.org.uk/media/pdf/f/q/1111_Workplaces_and_Social_Networking-accessible-version-Apr-2012.pdf**

[9] **http://www.huffingtonpost.com/alexandra-samuel/when-hr-decisions-become-_b_2664001.html**

[10] **http://harmon.ie/Company/PressReleases/press-release-may-18-2011**

[11] **http://www.websense.com/content/ponemon-institute-research-report-2011.aspx?cmpid=prnr11.10.06**

[12] **http://www.websense.com/content/ponemon-institute-research-report-2011.aspx?cmpid=prnr11.10.06**

[13] **https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200455/bis-13-p184-2013-information-security-breaches-survey-technical-report.pdf**

[14] **http://www.huffingtonpost.com/alexandra-samuel/when-hr-decisions-become-_b_2664001.html**

[15] **http://gizmodo.com/5954372/the-25-most-popular-passwords-of-2012**

[16] Burson-Marsteller Global Social Media Check Up 2012: **http://burson-marsteller.eu/innovation-insights/global-social-media-studies/**

“You only have to read about the increasing number of publicly quoted data breaches to see that an insecure system is not good for business.“

Chapter 11: Building a secure system: Why do we need to do it? How do we get it? And where should we start?

Chapter 11:

Building a secure system: Why do we need to do it? How do we get it? And where should we start?

Paul Hopkins, CGI

Abstract:

Whether an organisation builds software itself, integrates third parties or just procures a solution, the risks of a poorly secured system will ultimately have a significant impact on the business. Secure systems engineering, is not something that usually gets prioritised against the need to get to market quickly or reduce costs, unless of course the business truly understands the risks.

This chapter covers the risks arising from poor security engineering. We look at the potential impact on the business, what steps can be taken to mitigate these and therefore what questions all risk managers should be asking their internal and external architects and developers, highlighting the potential impact of software development methods such as AGILE on secure development methodologies.

Insecure Systems – Bad for business?

You only have to read about the increasing number of publicly quoted data breaches to see that an insecure system is not good for business. If you fail to keep your customers', or your organisation's, data confidential and available then potentially the consequences could be serious. The organisation could face a huge fine (e.g. TJ Maxx [8]), it could lose customers, it could get swallowed up by the competition (e.g. HBGary [7]) or it could contribute to the Company going out of business (e.g. Nortel [9]).

Not all of the publicly quoted examples above are just the result of an insecure system design and build, indeed social engineering of employees (alongside other factors) contributed to the end result. However, at the end of the day, the systems were compromised and exploited due to weaknesses in the overall system design that were not adequately assessed at the outset by the system designers.

It is possible you may be fortunate enough not to have your business put at risk as a consequence of a security breach. However, it is likely that the cost and difficulty of fixing the issues once discovered are substantially more than identifying and mitigating the issues earlier in the system development process. For a start, the problem may be within a third party component and it might not be possible to fix it directly yourself without their help. Alternatively the flaw may be in your software or technology so you might have the ability to directly address the problem. However, the problem may not be as simple as re-coding a file, e.g. it may be that the database you originally selected for its fast handling of queries has no way to adequately separate user data and therefore requires a new database technology! So, the scale and variation of the problem to be addressed once discovered can vary from quite minor to very significant, and that's without considering the additional operational impacts while you fix the problem (such as increased monitoring).

> It's not surprising that, given this rich stack of technology, (security) issues might arise either through the complexity of the application being assembled or through delivery pressure.

Secure Systems – Why it's hard

Securing systems is not trivial. An operating system has tens of millions of lines of code, a database server or a web server can contain several millions of lines of code. The software is resident on a complex mesh of servers, network infrastructure and multiple protocols on top of which the actual application is built that delivers the services which differentiate the organisation and provides value to your customers. So it's not surprising that, given this rich stack of technology, some 'issues' might arise either through the complexity of the application being assembled or through delivery pressures.

Unfortunately, such issues can quickly become security vulnerabilities. You only have to examine a number of prolific security industry reports [1], [4] to see that there are substantial numbers of vulnerabilities reported in web applications and enterprise software annually. There are also fewer but substantially higher impact year on year increases affecting software within technologies such as mobile platforms or Industrial Controller Equipment (SCADA). Of particular interest are reports which correlate vulnerabilities from internet facing web applications across a variety of industry sectors. In these we find common serious security issues, with one study [1] citing that 53% of all systems scanned contained a vulnerability that was potentially exploitable. Whereas a separate study of different applications [5] showed that 86% of the websites contained at least one serious flaw. So, if you take into account that such scans often check only for the 'known' bugs and flaws, then the question remains how many more latent security bugs and flaws that are not yet known are within such applications?

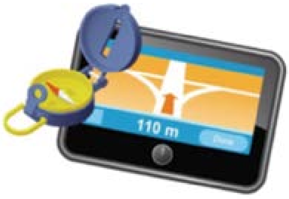
How can it be made secure?

The journey

The challenges of system complexity, pace of delivery and technology integration are not new to many organisations and development projects. Nevertheless, a number of organisations have successfully established secure design and development lifecycles as part of a prolific corporate commitment to reduce vulnerabilities within their products [14][15][16]. The lessons learned from these and other programmes have resulted in an increase in the techniques and guidance for secure design and development, with a corresponding improvement in secure systems [17] for those organisations that embed these techniques.

The following sections outline some of the key steps that should be used to secure systems.

A number of organisations have successfully established secure design and development lifecycles.



Security Requirements

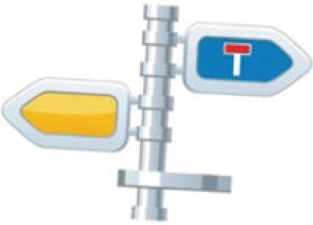
Plotting the journey

Clearly articulated security requirements are the starting point for any secure system development. These security requirements have to be related back to the actual system required by the business and its risk profile, and so are dependent upon the initial risk assessment for a system (or application), the threats, the potential vulnerabilities and the true impact to the business of the failure. This enables the subsequent secure development process to be tailored relative to the risk profile for the system, with the appropriate steps, quality and review gates.

If security requirements are going to be useful for subsequent development, then they need to be specific and not general statements such as "the application must authorise all users". It is far better to help the developers and designers with "the application must authorise users using the username, Memorable Word and PIN code". The requirement can then be further refined to constrain the subsequent functionality so that "each (web) page must check that a user's session is valid" and the "default behaviour is to deny access to all (web) pages without a valid session". Typically, this is not a quick exercise but elements can be re-used and their relationship to the business risks justifies their inclusion.

The form of the requirements need not be a pure specification document; indeed in previous projects CGI has found potential use cases or more precisely misuse/abuse cases have been helpful in communicating with system architects and developers the threats and risks to the system. The benefit is that the architects and designers clearly understand why they are implementing security controls and their relationship to the threats to the system rather than see them as annoyances that get in the way of implementing the business solution. Communication and collaboration between the business users, developers and security experts is essential to get the requirements understood and implemented as they are intended, rather than wait for disappointment at the end of the project.

With the requirements documented and an understanding of the application risk, the processes to be applied to the system development including the quality/security review gates can be defined and the next stage can be entered, which is to review the initial design.



Architectural Design

Picking the right road

Imagine this example, you are playing an online lottery game, you choose your numbers and you submit your bet then wait for the return of the results after a defined time period. You and the other customers are then presented with the winning numbers and you find out you've lost or you've won! More frequently you've lost. However, what if you noticed that the winning numbers were returned to your browser a few seconds before you were presented with the result and what if you found that if you re-submitted the bet with those returned results (very quickly after receiving the results) that you could change your numbers to the winning numbers and thereby win?

Actually this example was real but has long since been fixed and was an original flaw in the design of a gaming application. Yet it was also probably one of the simplest flaws where the designers incorrectly trusted the client (browser) with sensitive data in addition to not closing the lottery session before transmitting the numbers to the customers.

Unfortunately, such design issues are not always so simple and indeed not that easy to fix. The design issues can be caused by incompatible technologies or alternatively incorrect assumptions about the environment in which they will be working. Take for example the hospital software that pulls together a patient's records from different hospital departments with some records on file systems and others in databases. Here the designer has to carefully define the complex security rules (e.g. based on the user's role, the doctor's and patient's permission), how the application code implements these rules and also how those 'permissions' translate across the technology tiers: the database, operating system file systems and networks. If the security is only implemented within the application then the users may just navigate around it and directly access the records on the server. If it is at too low a level, such as within the network, then you won't be able to enforce complex security policies.

In which layer do we trust?

Systems are composed of multiple software layers, often dependent upon the others for certain functions, including security. Assumptions about these layers and about how they will be configured or used can often undermine the overall system security.

One such security issue, that's frequently proven to be problematic, is the use of cryptographic libraries (such as TLS/SSL) [2]. A recent study [11] on an Android platform demonstrated the inadequate 'certificate' checking by banking applications (amongst other applications) to validate and setup a secure channel between the device and the organisation's application, leaving the users vulnerable to interception[16].

[16] In reality such an attack also requires the subversion of some of the components of the network infrastructure between the user and the application (such as on a wireless network), but then the server certificates were used as a secondary protection mechanism to ensure only the authentic application is being communicated with.

More disconcerting was that 26% of all (29.8 million) library downloads contained vulnerabilities.

A second issue is the assumption about the number and frequency of vulnerabilities that may be latent within the libraries and frameworks that you use as part of your system. For example, a recent study by an application security company [3] found that 37% of the most popular frameworks and libraries (used primarily for building web based applications) contained at least one vulnerability. Possibly more disconcerting was that 26% of all (29.8 million) library downloads contained those vulnerabilities. This problem is increasingly likely in mobile devices where libraries, such as Webkit, have been shown to contain serious flaws affecting the integrity of a number of mobile (browsers) and subsequently the devices themselves.

A third security issue is the introduction of malicious code into the system or where perhaps that application becomes malicious (i.e. once deployed). Mobile applications often have integrated (via a Software Development Kit) connection to advertising, in order to generate revenue. Unfortunately, some such benign apps have also been discovered to connect back into a malicious ad network (such as BadNews [13], [10]) that will serve up malware potentially compromising the customer's device.

Fortunately, there are a number of steps that the system designers should be going through at this stage to avoid such failures.

Architecture Checklist:

1. Independently analyse the system design against specific threat or attack patterns. Microsoft's STRIDE is one such generic pattern frequently used to stimulate that process, but it's also important to look at the specific threat patterns within your industry, e.g. for banking and retail applications the 'man in the browser attacks'.
2. Look at the technologies used and understand where there may be incompatibilities, particularly with security controls such as cryptographic libraries/APIs and access control. Alternatively, as is the case for mobile development, the design may be considering using common functionality to develop applications (HTML5/Javascript) that may undermine the security on specific platforms. Or it may use the specific mobile platform toolkit that may initially make the design stronger, but will need any operational platform patching to be carefully considered to avoid applications on one platform being patched while there is lag in fixing the other platforms.
3. Understand and capture how the architecture is built up. How and where the important data flows and is stored? Where the security controls are placed? What assumptions are being made at the network, in the operating system, in the application (and its software stack of libraries/frameworks) and what assumptions are we making about the user and their environment.

We might suppose that our corporate environment is free from hardware or network level attacks but you only have to look at recent news reports of such attacks on retailers and banks [6] to realise that we may need to check that assumption.

4. Verify and understand the design and assurance of all the components. How have they been developed? How have they been validated or tested? And how are they being used? For example, have you tested the applications and components according to your standards? Do they have any third party assurance (and what confidence does that give?). As per the previous examples do our developers understand the risks, issues and mitigations and are they using the APIs or applications in the right way?

5. What is the provenance of the components and applications? Understand how the components to be used have been or will be built. Will you be able to understand who has had access to the code? For example, has the code been hosted on a potentially insecure public cloud with limited auditing and weak access controls to the code? Have they been developed, tested and managed in a way that we know is free from tampering?

Develop & Test

Avoiding damage along the way?

Returning back to our previous online gambling example, imagine that the flaw has been fixed and instead of winning you find yourself losing every time and the account balance dwindles away. However, what if now you were allowed to submit varying amounts of money for each bet and instead of betting positive values you entered negative numbers? You might be surprised to find that another real (but now fixed) application instead of debiting your account every time you lost, credited the balance by the same (negative) number bet, thereby increasing the account balance!

While this could arguably be considered to be a logical flaw, it demonstrates one of the most basic security mistakes made by developers – essentially "trusting the input". Indeed many of the most serious vulnerabilities discovered in systems software are caused by trusting input, be that from a user, another application or a network protocol/packet. But this is only

one potential development issue, there are also many other types associated with web applications (Cross Site Scripting (XSS), broken authentication mechanisms, forced browsing etc), with databases (SQL injection), within the code in operating systems (such a buffer overflow, race conditions).

However, unlike the earlier design flaws, these programming errors can be more readily addressed during the development process by the programmer, as long as they are provided with the right tools, process, standards and training.

Development Checklist:

1. Coding standards have been defined and the code is checked to ensure it adheres to those standards and is understandable for maintenance purposes. Automated tools can be used to check code against the defined standard (e.g. checkstyle).
2. Train the developers to write secure code, by understanding common attack patterns, such that they validate and sanitize input or use trusted security APIs from organisations such as OWASP. For instance there are increasingly good guidelines for mobile application development from both the manufacturer (e.g. Apple) and governments (CESG [12]).
3. Train and give the developers access to both security testing tools (e.g. those used to test and manipulate protocols and application input) as well source code analysis tools for potential security flaws. Some of the analysis tools can be run outside of working hours to reduce the downtime for development.
4. Ensure that the team has a security champion within it, someone who is prepared to mentor (and train) other team members, help resolve security questions and share best practice/ lessons learned.
5. Use the output of automated tools (or third party services – including those embedded within mobile app stores) such as source code analysis to look for common recurring problems that might indicate that developers don’t fully understand certain issues and use this to focus the ongoing training and sharing of best practice.

Assurance

Ready to proceed?

So you've articulated your security requirements and you've translated them into a security architecture. You've then developed the system (encouraging the developer to use security testing and source code analysis tools) during the development process. The last stage is to focus on the real world security testing, where the application or system has been integrated and all of the components in the system must be tested together to check that the security controls work.

This includes creating tests based on:

a) The original security requirements e.g. does the application stop us browsing to another users bank account summary when we aren't authenticated?

b) Common security issues e.g. does the application stop us injecting commands into the application to extract from or put information into the database? Has the data been stored in the mobile device using encryption?

c) Specific applications or specially developed security controls e.g. does the system interface work with the cryptographic module/library correctly and does it handle and present the challenge/response for the pin pad correctly?

Third party software should be of particular focus as it may itself contain bugs or be incorrectly configured when used with the rest of the application stack. Unlike the code the organisation has developed, it may not have been subject to an architectural review and constant testing while in development. Additionally, it may require testing for the presence of malicious applications or software as per the earlier mobile example [13].

Particularly for mobile applications, the security testing should be supplemented with additional steps to review the open-source meta-data about the application and developer (i.e. to establish how trustworthy they are). This should be followed by a local analysis of how the data and device capabilities accessed, along with a source code and network analysis.

In most instances, an independent team of testers best perform this step. The broader the experiences of the security testing team (within and outside of your industry sector) the better the testing result.

Developing the skills and security culture is one of the most important activities needed to develop a secure system.

Security Culture & Skills:

Setting the tone

Developing the skills and security culture is one of the most important activities needed to develop a secure system. All of the people involved in building the system must believe that a secure system is worthwhile, and not only will it protect the business and the customers, but also they must have the right skills and training to achieve it. It is also something that must be right at the inception, throughout the project and long after it is completed and embedded into the team.

So far in this chapter the focus has been on designers and developers, yet in reality, when it comes to constructing a system, we need to know that many of the roles involved (e.g. project managers, contracts, business managers) all believe in the value of the steps outlined. Otherwise they may be tempted to trade-off without understanding the implications – "early delivery rather than compete security testing" or "choose not to check third party secure development practices before purchasing for cost reasons" or "perhaps not check the identity of all users in the interests of usability".

Creating a security culture is not an easy thing to achieve, especially if you have a diverse or large geographically distributed organisation. However, CGI has found the focusing on the following steps helps:

1. Getting buy in from senior stakeholders early and clearly articulating the benefits to them.
2. A clear message from the senior stakeholders disseminated to the rest of the organisation.
3. Focused training for developers (on security vulnerabilities/common patterns and security test tools).
4. Giving frequent feedback to the developers and using it to refine the training of the existing development or next generation team so that the lessons learnt are not lost. Be careful to capture and manage this knowledge with incoming or new suppliers and teams otherwise you may find yourself starting from scratch all over again.
5. Giving frequent feedback and communicating with the rest of the 'development' team on the security progress. The benefits and successes, such as the number of bugs and flaws avoided through design and development reviews and testing.
6. Include security in reporting mechanisms. Staff and managers will always respond to what they are measured on.

Changing Landscape

Increasingly, for many organisations, the software development lifecycle has been compressed and changed from what were once monthly cascading (or waterfall) phases to now weekly updates with daily stand-ups and an iterative and rapid software development (AGILE) process.

A number of organisations have needed to adopt AGILE to increase the pace of development for the organisation and have integrated the security lifecycle steps presented earlier in the chapter. For example, while some AGILE processes are well suited to integrating security, such as the code development phase with its rapid development and iterative testing, by contrast the architecture analysis can seem at odds with the iterative nature of AGILE. The reality is that design reviews and code clean-up need to be added to the backlog to become part of scheduled sprints. Of course in order to get these activities onto the backlog, you still have to use the user stories to develop and articulate the security requirements, either by establishing them around the functionality required or alternatively as a constraint upon that functionality. Requirements particularly need to be given sufficient priority so that they don't fall below the achievement line of each sprint. Given the rapid nature, individual sprints must focus on completing the most relevant parts of the previously described steps (e.g. design review, testing, code analysis) rather than attempt to tackle all of the steps within one sprint.

However, the key to establishing any secure development is still to get user buy-in and appropriate prioritisation of these activities by the team.

Final Thoughts

Based on CGI's experiences there is no quick route to building a secure system. However, as CGI and many other organisations have found, by focusing on the key steps within this chapter, you can significantly increase the chances you will achieve a secure system and may also decrease the overall cost of development.

The security requirements are the starting point, linked to the enterprise risks and threats from which a system can be developed. These requirements need to be proportionate and relevant to the risk, e.g. a mobile application can have a very different set of requirements to that of an internal facing web application.

Eliminating significant flaws during the design or architectural review stages ensures you don't face 'insurmountable' security problems once the system is deployed or just prior to deployment. By contrast, the secure development practices and independent security testing should enable the development team to produce a quality product with minimal bugs that are also less costly to fix once a system is 'live' and with customers.

> The key ingredient is ensuring that you have established the secure development practices as being relevant and 'alive' within the organisation.

However, the key ingredient to all of this is ensuring that you have established the secure development practices as being relevant and 'alive' within the organisation:

- You have established and defined the development process so that it is repeatable, constantly improving and adapting to the business.
- You have gained and continue to receive support from the management and organisation (based on improved security results! – remember to measure).
- You have focused on your organisation's needs (the technologies used, the supply chain/partners, the agility needed) and most importantly the risk the organisation is prepared to accept.

Top 10 questions to ask of your organisation:

1	Do you follow a defined process to build secure systems? Have you defined the appropriate review/quality gates?
2	Do you have the support of senior management, Project Managers, Contracts and Developer teams for a secure development process?
3	Do your suppliers understand and support this process?
4	Do you regularly and clearly identify the realistic threats and risk to system data and functionality?
5	Have you provided clear security requirements that can be tested against?
6	Have you independently reviewed the architecture? What threats have been modelled? Do you understand how the system protection works across all technology? What assumptions have been made about the environment and ongoing operations/maintenance/customer interaction with the system?
7	How have you developed the code? Have you defined secure coding standards? Have you trained your development teams to understand the key risks and threats and how to protect against them? Have you given them security testing tools and source code analysis tools to check for problems?
8	Do you conduct independent testing that simulates real-world attacks?
9	Do you measure and feedback regularly the results and lessons learnt from testing and source code analysis into developer training?
10	Are you developing the right skills and culture to consistently build secure systems? Do you have the right security champions in place?

References

1. *2013 Internet Security Threat Report, Volume 18*; **http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf**

2. *The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software*; M. Georgiev et al; 2012; **http://www.cs.utexas.edu/~shmat/shmat_ccs12.pdf**

3. *The Unfortunate Reality of Insecure Libraries; Aspect Security*; March 2012 **http://cdn1.hubspot.com/hub/203759/docs/Aspect-Security-The-Unfortunate-Reality-of-Insecure-Libraries.pdf**

4. *HP 2012 Cyber Security Risk Report*; 2012; **http://www.hpenterprisesecurity.com/collateral/whitepaper/HP2012CyberRiskReport_0213.pdf**

5. **https://info.whitehatsec.com/2013-website-security-report.html**

6. *Scammers bug retail registers with $40 keylogger devices;* SC Magazine; October 2013; **http://www.scmagazine.com/scammers-bug-nordstrom-registers-with-40-devices-to-skim-card-data/article/316001/**

7. *Anonymous speaks: the inside story of the HBGary hack*; Ars Technica; February 2011; **http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/**

8. *TJX, Visa Agree to $40.9 Million Payout for Data Breach*; BankInfoSecurity; **http://www.bankinfosecurity.co.uk/tjx-visa-agree-to-409-million-payout-for-data-breach-a-648**

9. *Chinese Hackers Suspected In Long-Term Nortel Breach*; Wall Street Journal; February 2012; **http://online.wsj.com/news/articles/SB10001424052970203363504577187502201577054**

10. *Bad News for Android as Fake Ads Target Google play; Mobile World Live*; April 2013; **http://www.mobileworldlive.com/badnews-for-android-as-fake-ad-network-targets-google-play**

11. Attackers can slip malicious code into many Android apps via open Wi-Fi; ArsTechnica; Sept 2013; **http://arstechnica.com/security/2013/09/attackers-can-slip-malicious-code-into-many-android-apps-via-open-wi-fi/**

12. *End User Application Security Guidance for iOS*; CESG, November 2013; **https://www.gov.uk/government/publications/end-user-devices-security-guidance-apple-ios-application-development/end-user-devices-security-guidance-apple-ios-application-security-guidance**

13. "*Mobile Devices = New Malware and New Vectors*"; Palo Alto Networks; August 2013; **http://researchcenter.paloaltonetworks.com/2013/08/mobile-devices-new-malware-and-new-vectors/**

14. *Cisco Secure Development Lifecycle; Cisco;* Retrieved November 2013; **http://www.cisco.com/web/about/security/cspo/csdl/index.html**

15. *Oracle Software Security Assurance; Oracle;* Retrieved November 2013; **http://www.oracle.com/us/support/assurance/overview/index.html**

16. *Microsoft Security Development Lifecycle; Microsoft;* Retrieved November 2013; **https://www.microsoft.com/security/sdl/default.aspx**

17. *The Trustworthy Computing Security Development Lifecycle. The Benefits; Microsoft;* March 2005; **http://msdn.microsoft.com/en-us/library/ms995349.aspx#sdl2_topic4**

Do you measure and feedback regularly the results and lessons learnt from testing and source code analysis into developer training?

> “This chapter aims to provide guidance on effective incident management in response to cyber related events.”

Chapter 12: Incident management

Chapter 12: Incident management

Alastair Allison CISM SIRM and Jeff Miller

Abstract

This chapter aims to provide guidance on effective incident management in response to cyber related events. It will examine incident management from both the technical perspective where network and internet facing detection controls are present and also from a management perspective where significant events could harm customers and the organisational reputation. We will consider the five phases of an incident and discuss the possibility of data sharing between organisations to help defeat the increasingly organised nature of cyber criminals. For the purposes of this chapter, we define an information security incident as a violation or imminent violation of information security policies, acceptable use policies or standard security practices.

Introduction

100% security cannot be achieved no matter how much we invest. Zurich and the On Line Trust Alliance (OTA), among others, state that "suffering a data breach is now almost inevitable" and evidence in the press, cyber security surveys and on the internet show that the number of reported information related incidents is growing at an alarming rate. Whilst some of these can be put down to mandatory reporting requirements in some countries, it cannot be the primary factor. NIST (2012, p10) reminds us that performing incident responses effectively is a complex undertaking. Consequently, it is important to have a robust incident response procedure with appropriate statements in place to minimize the damage if, or when, an incident should occur.

True resilience needs effective incident management protocols in place and capable of being operated at different management levels. Operating in a dynamic, often high pressure environment making rapid decisions or even reversing decisions, requires a certain type of character for it to be successful and not everyone is best suited to leading in a crisis situation. However, as mentioned in the governance chapter, clear leadership and accountability is crucial and it needs to be understood before an incident takes place. It is also crucial for those in the regulated environments, as effective incident management can have a positive influence on the regulators investigative decisions and in considering any remediation actions or fines to be applied.

Case Study

Following the hacking attacks on Sony in 2011, there was a 24% fall in its share price over a 3 month period, the CEO had to apologise to the Annual General Meeting and took a 16% cut in pay as chief executive

Source: FT.com/comment

> 100% security cannot be achieved no matter how much we invest.

The risks

The major risk arising from not having incident management procedures in place is one of reputational damage. “Organisations should develop a taxonomy of risks and potential failure modes and develop easily accessible quick response guides for the likely scenarios” (Bailey and Brandley).

The most likely risk events in terms of Information security and incident management are considered below.

Preconditions	Event(s)	Risk(s)
Management do not support the need for prepared incident responses trusting in their instinct to react appropriately to any event.	1. There is a data loss not detected by the organisation. 2. The organisation suffers a cyber attack. 3. A data loss is reported on social media /to the press by a victim unsatisfied by the organisational handling of the loss. 4. Response to media interests is perceived to be inappropriate leading to further press interest. 5. Regulator supervisory action taken on the organisation. 6. Organisation is fined by a regulator.	There is a risk that the organisation’s reputation is damaged affecting customer trust to protect their data and a consequent impact on revenue and/or share price (private company) or service delivery (public company) and the time to recover becomes protracted. See chapter 4 for more detail on the iceberg impact of an incident.
Weak information security control environment that is unable to detect breaches.		
Staff are unaware of media relation procedures.		
Non-existent or poorly communicated incident reporting procedures.		
Incident management team not trained or suffer high levels of turnover.		
Incident response plan is too detailed and complex for people to quickly refer to it in a crisis.		

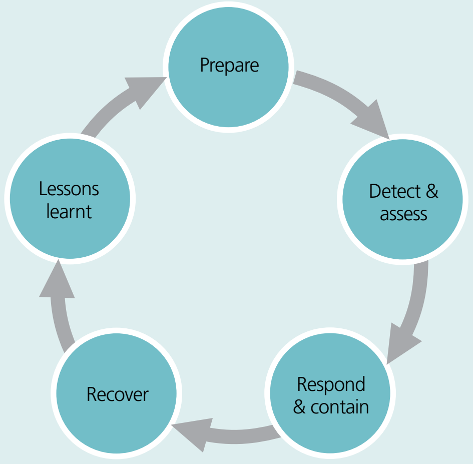
The benefits

Organisations that have established Business Continuity Management (BCM) procedures such as the ISO25999 will be acutely aware of the benefits of forward thinking the disruption scenarios. Effective risk management should be able to predict the majority of business disruption scenarios against which an organisation can make preparations or establish fallback plans and business continuity plans and cyber security is no different. The goals of a structured and rehearsed incident management approach can be summarised, according to ISACA (Chapter 5 p250) as:

- Detect incidents quickly
- Diagnose Incidents accurately
- Manage them properly
- Contain and minimise damage
- Restore affected services
- Determine root causes
- Implement improvements to prevent recurrence

Additionally, incidents that have been managed, assessed and reported on offer new insights to the effectiveness of the information security framework (Humphreys, p87) in place such as new weaknesses and threats, the effectiveness of security controls or defects in those controls and analysis of business impact assessments. In the final analysis, a good incident management and response process will allow an organisation to effectively deal with unanticipated and potentially damaging events in a controlled manner that facilitates more effective decision making in a crisis. Finally, as part of a wider risk mitigation strategy, organisations should benefit from reducing the frequency and severity of incidents and enhance their reputation for effectively managing incidents should they occur.

Figure 12.1: Phases of Incident Management



Who has the responsibility/ authority to declare an incident?

The key steps

Literature used in this research suggests that there are between four and six phases of the incident life-cycle. However, they all tend to agree on the key components and we represent these in our five phases on incident management shown in Figure 12.1. The most crucial of which is probably the "Prepare" phase.

Incidents, by their very nature tend to be fast paced. An airline pilot is trained to handle an aircraft in crash-landing scenarios yet hopes to never use that training. Nevertheless, such training has saved countless lives as the training allows the pilot to respond with some familiarity to procedures rather than having to think on their feet in a crisis. In very much the same way, examining potential crisis scenarios involving data losses will help organisations prepare response plans which can be rehearsed so that the chances of a successful outcome are maximised. The next few paragraphs describes each of these five phases in a little more detail.

Preparation Phase

Documentation

Appendix 12.1 – Incident Management Checklist looks at the key steps required to define the preparatory work that has to be completed to cover the before, during and after incident contexts such that the processes can be put in place. NIST (2012, p11) highlights that not only should these preparatory actions be documented but that there should also be documented guidelines for interactions with other organisations regarding incidents including all the contact details and the facilities to be put in place such as phones (NIST p31).

Rating incidents

NIST also highlight how there should be guidance on prioritising incidents according to the risk severity. Incident levels could be tiered such that:

- Tier 1 – Localised/internal breaches or attempted external attacks that can be easily isolated and contained through local management actions. Such breaches may also affect a single customer and are unlikely to warrant regulator attention.
- Tier 2 – Unusual and immediate threat such as a deliberate/persistent attack or breach that could harm large numbers of customers and the reputation of the organisation and requires key decisions to be made by senior executives or managers to contain and bring under control.

Accountability and Responsibility

A key component of the preparatory phase is to identify who has the responsibility/ authority to declare an incident and the team members that would respond to it. The team should be a small group committed to solving the problem and mitigating any damage that it may cause. Consequently it will need to have people with certain skill sets, experience and authority "to respond to incidents, perform analysis tasks and communicate effectively" (ISACA, p260) to make a rounded response and it may also include external parties such as public relations or legal expertise. Usually there will be a core team that is augmented by specialists according to the specific context of the incident. Such a team may be a centralised team or distributed such that virtual working mechanisms have to be put in place including conference facilities.

A recurring thread through-out all phases is the need to communicate in a manner that protects the interests of the organisational aims and, where appropriate, the victims of the incident.

Testing/war gaming

Any good business continuity practitioner will tell you that incident plans are not worth the paper they are written on if they are untested. Cyber incident scenarios should be built in to the BCM testing regime and rehearsed. Lessons will be learnt about the best way to handle situations or about the composition of the incident team and these should be smoothed out before an organisation needs to do it for real.

Immediate actions

Upon forming in response to any incident, the immediate actions of the team would be expected to be to:

- Conduct a risk assessment
- Contain the breach
- Recover the data
- Communicate and notify appropriate stakeholders
- Investigate the incident
- Identify improvement mechanisms including addressing the root cause.

Communication

A recurring thread through-out all phases is the need to communicate in a manner that protects the interests of the organisational aims and, where appropriate, the victims of the incident. Law Enforcement agencies and the media should be "contacted through designated individuals" (NIST, p20) and for regulated industries there are usually Approved Persons that notify breaches and incidents to the regulator. These need to be identified and staff need to be aware of the contact procedures involved if the incident is to be effectively controlled.

Log of activities and costs

Likewise, those organisations that have cyber insurance may have a requirement capture certain information such as costs or response logs and times and to notify the potential losses within a determined timeframe. The person who should have responsibility for this needs to be identified in advance and templates to track costs and mitigating activities need to be prepared in advance.

Detect and assess

The following section is a case study from a global insurer who, whilst they do not exactly fit the 5 phase model described in this chapter, do have all the key components in place.

Technical logs and detections

Key to timely detection at the technical level is the ability to aggregate log events and raise specific events to the attention of handlers. The primary drawback to this is the sheer volume of events generated within a large enterprise and the maintenance and updates required to specific "events of interest" which will be escalated.

A two pronged approach is recommended with critical devices, such as perimeter firewalls, IDS/IPS devices, logged to an active security event monitoring platform and secondary, or contextual device logs (routers, switches, domain controllers, application logs), being aggregated to a central logging warehouse for future reference and/or analysis. This approach reduces the amount of data that must be sifted for primary alert triggers yet provides a means to research the context around these events.

First level "log sifting" is accomplished in an automated fashion using basic string searches across the active log streams. Log rates and volumes are also monitored by the automated system and are used for system diagnostics as well as security alerts. A device changing logging rates may indicate an event of interest.

Once an event is identified as "interesting" it is escalated to a trained "event handler" to confirm or collect ancillary information to determine the type and severity of the event (or series of events).

Once it has been determined a security incident has occurred, response activities typically fall into the phases of Analysis, Containment, Remediation, and Post-Incident.

- **Analysis** – Steps taken to better understand the incident and its impact to systems or information. This determines the scale of the incident as well as the categorisation and criticality.
- **Containment** – Engagement of the proper teams to prevent further spread of the incident. The closure of the initial attack vectors, identification of necessary remediation actions, and gathering of evidence for forensic purposes as necessary.
- **Remediation** – The actions taken to prevent a recurrence of the incident on the target system and other similar systems within the environment. This includes the cleanup of any remnants of malicious activity which occurred during the incident.
- **Post–Incident** – This includes the determination of lessons learned through the creation of an After Action Report if necessary. Modifications to the monitoring, detection, or response processes or capabilities are identified and implemented if required.

Actions and escalations

The specific actions and escalations taken during each of these phases is dependent on the type of incident as well as the criticality of the systems impacted:

- Incident category examples:
  - Commodity malware
  - Hacking/exploit tools
  - Privilege escalations
  - Reconnaissance
  - System exploits
- Characteristics affecting criticality:
  - Criticality of the systems
  - Data staging/exfiltration
  - Impacts to system availability
  - Fraud

Externally reported incidents

Incidents may not be purely technical and may occur outside the logging process discussed above. According to Verizon, 85% of breaches are notified from outside the organisation and there needs to be agreed processes for dealing with such incident so that they are handled by the right people in a timely manner. The approach to dealing with these is not too dissimilar to that discussed above but once an incident has been identified, organisations should assess a number of factors before trying to respond and contain any further damage.

The Incident team should be set up with the objectives shown above. However, part of the risk assessment must be derived through knowledge of what has happened based upon established facts. Appendix 12.2 – Incident Evaluation Initial Checklist offers a format for this purpose. However, organisations that already have an established Business Continuity Framework under ISO25999 should look to integrate responses to information security breaches/incidents into existing practices so to minimise any resistance to change.

Respond & contain

Maintain a log

Maintaining a log book for the incident is important. Key events can be poured over at regular intervals and kept fresh in everyone's mind. During a crisis, new thoughts and ideas come to mind as new information presents itself to the team. Having all the information and decisions recorded and available is important not only to review what was done but why and also to understand the rationale for retracting any of the previous decisions. Teams should also be mindful that the data and the evidence is likely to be sensitive (NIST, p31) and so need to be adequately protected and verified as true copies with originals secured away from any form of manipulation or tampering (admissibility of evidence has to be assured).

Initial actions are key to long term success

The initial actions taken to respond to a detected breach/incident and the efforts to contain the damage will prove to be crucial in any legal defence action. Appendix 12.1 – Incident Management Checklist provides the breakdown of what is required to be done during the incident itself. There are essentially two key areas of focus: warning potential victims based on the facts and preventing further loss/abuse of the data. The former focus area is a fine balancing act between being too early and inducing ill-informed panic or too late and so well informed that further damage limitation is unlikely. Organisations should consider the loss scenarios and during the rehearsal of its response, test the logic of the team decision making to ensure it will be appropriate and meet regulatory expectations.

Incidents may not be purely technical and may occur outside the logging process.

Contain it!

"Containment is important before an incident overwhelms resources or increases damage. Most incidents require containment, so that is an important consideration early in the course of handling each incident" (NIST p35). Containment will also be a management judgement as to what reasonable steps have to be taken. In the Supply Chain chapter, there is a case study that involved an organisation taking legal proceedings out in three jurisdictions simply to contain the spread of a data theft being sold in the market. They also felt it was reasonable to employ a private investigator. Each organisation will assess the risk according to the data but the involvement of external stakeholders during a breach such as law enforcement should not be overlooked in the preparation phase so that reporting requirements can be duly met. Bailey and Brandley suggests that this means maintaining "service level agreements and relationships with breach remediation provider and experts" or at the very least, identifying who needs to be contacted and how. Response teams should become acquainted with the conditions under which law enforcement should be contacted and incidents are reported to them. NIST (2012, p11) point out that poor conviction rates for cyber-security incidents is down to organisations that "do not properly contact law enforcement" agencies.

Containment also includes co-ordinated messages to victims, the media and other customers/clients and these should also be rehearsed before they are used for real.

Recover

Recovery occurs after the incident and Appendix 12.1 – Incident Management Checklist discusses some of the detailed components to consider. Recovery involves restoring systems and processes to normal operations including the implementation of any remediation actions to prevent a re-occurrence. NIST (2012, p37) term the phrase "Eradication and Recovery" for this phase pointing out the need to also eradicate things like malware and breached user accounts which is useful to consider but in essence, that could have either been achieved during the "containment" exercise or is central to recovery with such activities as applying patches, changing passwords etc.

Organisations need to consider that a successful attack may be followed by a subsequent attack on the same resource or system or that the same attack method may be used on other systems so part of the recovery is to put all remediation in place and to increase detection and monitoring. However, remediation can be both large and expensive and it will be necessary to take a risk based approach to any remediation plan with the intent "to increase the overall security with relatively quick (days to weeks) high value changes" (NIST, p37).

Processes also need to be reviewed and changed but our research suggests that organisations are not always good at applying the fixes or to validating that they are still working sometime after the event. As with any risk and control activity, the controls need to be assured for design and operating effectiveness according to the criticality of the process not just at the point of implementation. We would contend that if an incident has warranted the instigation of a response team, new controls should be reviewed within the first 12 months to give assurance that the incident has a reduced likelihood of re-occurring.

Finally, as is discussed in the Insurance Chapter, certain costs can be recovered through cyber insurance and the recovery process needs to ensure that the costs are calculated and maintained ready for submission to the insurance carrier.

Lessons learnt

The final phase is to have a wash-up of the events. This meeting aims to pull the response team together to affect closure and review what went well, what did not and set about a virtuous circle of process improvement. This should also consider staff behaviours, ability to respond to stressful situations and the leadership involved. It should also aim to see if any useful early warning indicators can be identified to detect such an incident at a much earlier stage. By doing so, the organisation might be able to identify ways of reducing future costs. The level of analysis will depend upon the severity of an incident and how widespread it was felt across the organisation and supply chain. However, the key components of a closure report are suggested at Appendix 3 – Post Incident Closure Report.

Knowledge share

The EU, UK and US are leading calls for increased co-operation mechanisms to share early warnings on cyber risks and incidents. Businesses are being encouraged to share incident data so that they can learn from each other. However, the IRM survey on this topic saw a marked decline in respondents to the incident section by over 50% of all respondents. Indeed, of those that did reply less than 3% were prepared to share data on their incidents and even then the sharing was on a limited basis. The gap, therefore, between the political aspiration for data sharing and the preparedness of businesses to do so appears to be a big one to overcome. Nevertheless, there are already some forums committed to knowledge sharing of cyber management and also of incidents. Whilst these appear to be contained to specific sectors, it is a step in the right direction.

Cyber risk is never a matter purely for the IT team.

The success of the internet is down to its ease of use and lack of controls yet these strengths are also its weaknesses to provide a safe and open trading platform. The criminal activity still follows the money but instead of being in bank vaults, the money can be gained from on-line activity. Better intelligence and data sharing among businesses will help in the fight against cybercrime by raising the barriers to successful attacks and also help reduce the number of cyber incidents that businesses need to respond to. Organisations should, therefore, consider industry specific forums to share knowledge on incidents. In doing so they may prevent the same incident happening elsewhere in the supply chain in our ever inter-connected world.

Conclusion

"Putting the development of a robust plan on the fast track is imperative for companies. When a successful cyber-attack occurs and the scale and impact of the breach comes to light, the first question customers, shareholders, and regulators will ask is, "What did this institution do to prepare?" (Bailey and Brandley). True resilience needs effective incident management protocols to be in place and able to be operated at different management levels according to the severity of the risk to the organisation. Risk managers and audit professionals need to determine if their processes are truly robust to respond to a cyber-attack in a timely manner to protect the organisational reputation as well as minimise the harm to the customers/clients affected by the crime.

Reading list and websites

1 Bailey, T and Brandley, J, Jul 2013, *Ten Steps to Planning an Effective Cyber-Incident Response*, Harvard Business Review accessed via **http://blogs.hbr.org/cs/2013/07/ten_steps_ to_planning_an_effect.html** on 12 July 2013

2. Humphreys, E, 2010, *Information Security Risk Management Handbook for ISO/IEC 27001*, BSi

3. ISACA, 2011, *Certified Information Security Manager Review Manual, Chapter 5*

4. NIST SP800-61 Revision 2, 2012, *Computer Security Incident Handling Guide*

5. *Online Trust Alliance 2013 Data Protection & Breach Readiness Planning Guide* accessed via **https://otalliance.org/resources/Incident.html** on 23 July 2013

6. Zurich Insurance Group, Insights magazine – *Security and Privacy Risks*, accessed via **http://view.pagetiger.com/ZurichInsights/SecurityandPrivacyRisk2012/** on 23 July 2013

Appendix 12.1

Incident Management Checklist

When a breach occurs it is important to deal with it quickly and efficiently to minimise any impact to those affected and to the organisation. Being prepared before the event allows organisations to not only respond but continuously improve their processes and learn from others. Use the checklist below to assess your organisational readiness to deal effectively with any data breach.

Before: **Pre-breach preparation**	
Identify team members – who should respond and how often should they meet?	
Monitor the systems – how will you know if a breach occurs?	
Data Collection – How do you review how you collect data, including 3rd party data, cloud services and subsequently audit it?	
Classify the data – If any data is lost will you understand the potential impact based on its classification and the level of protection it needs to be afforded?	
Data Storage – Where is the sensitive data held, stored or archived and are there adequate controls in place?	
Training – Are staff trained to report breaches and are the team members trained in how to handle a breach?	
Escalation – Are the escalation routes clear according to the severity of a potential breach?	
Regulatory Authorities – Are you aware of any regulatory reporting requirements and timeframes?	
Specialist Support – Will you need specialist service providers/advice in the event of a breach such as public relations, risk engineering, eDiscovery and forensics?	
Communication – Is the organisation ready to communicate with customers, partners, stakeholders and the press in the event of an incident?	
Documented Plan – Is all the above in a documented plan or process flow?	

During: **Dealing with a breach**	
Assess the situation What, where, when and how? Who knows? What action has been taken and by whom?	
Notification Who needs to be informed within the organisation? Who can help? Who can make the appropriate decisions?	
Containment Confine the damage and spread of the breach	
Victim notification Many jurisdictions require that victims have to be notified within a set time frame. However it is simply good practice to notify and limit the harm to others.	
Call centre Establish a central call centre and information page where potential and actual victims can find out more about the breach and what they need to do.	
Credit/Identity monitoring & fraud remediation service Consider setting this up depending on the circumstances of the breach.	
Public relations Have statements ready to restore your reputation and show that you are in control.	
Legal defence How will you defend yourself in court or with regulators?	

Appendix 12.1

Incident Management Checklist

After: **Post breach activities**	
Notify affected customers Ensure the information is accurate, efficient and timely and includes advice on how to limit further losses/harm.	
Public relations Ensure the PR team continue to monitor and respond to the fallout and that messages are consistent.	
Funding and insurance Establish the cost of remediation, what is covered by any insurance policy and the budget required to prevent a recurrence.	
Notify regulators Ensure all relevant regulatory authorities are notified and kept up to date with open and transparent communication as applicable.	
Post-incident review Establish a review team to investigate the root cause of the breach, identify lessons learnt to prevent re-occurrence and to improve future breach handling procedures.	
Validate new processes Validate that lessons learnt and any revised processes have been adopted into normal business operations with a review within 12 months of the incident.	

Appendix 12.2

Incident Evaluation Initial Checklist

Once an incident has been detected, quickly understand what has happened and help determine what actions need to be taken by following this quick agenda.

Incident evaluation: **Initial agenda**	
WHAT has happened?	
WHEN did it happen?	
WHERE did it happen?	
HOW did it happen?	
CONFIRMATION that it has happened?	
IMPACT of what has happened?	
Victims – and what has been done for them?	
Actions taken so far?	
Who has been notified and who remains to be notified?	
Estimated time to recover?	
Potential for escalation of incident?	
Actions needed?	
Other information?	
Next report expected when?	

Appendix 12.3

Post Incident Closure Report

A full and proper review of the incident should occur including a root cause analysis so that process and behavioural improvements can be made where appropriate. It can also provide regulators with the necessary information they need to assess the measures taken by the organisation to prevent a re-occurance.

Post incident report format
1. Introduction
2. Initial events and circumstances
3. Actions taken • Workstream 1 (e.g. customer, regulatory, investigation, business etc) • Workstream 2 • Workstream 3 etc…
4. Findings
5. Processes to be amended
6. Lessons learnt (incident handling)
7. Conclusion

OCTYPE HTML>
f lt IE 7]> <html class="ie ie6 lte9 lte8 lte7"> <![endif]-->
f IE 7]> <html class="ie ie7 lte9 lte8 lte7"> <![endif]-->
f IE 8]> <html class="ie ie8 lte9 lte8"> <![endif]-->
f IE 9]> <html class="ie ie9 lte9"><![endif]-->
f gt IE 9]> <html> <![endif]-->
f !IE]><!--><html> <!--<![endif]-->
Sell your photos and make money">
photography, photos, digital, royalty free, images,
Sell your photos and make money"> <meta name="k
<head>
<title> Earnings Summary</title>
<meta name="description" content=" Sell your photos and make money">
<meta name="keywords" content="sell stock photography, photos, digital, royalty free, images,
eta NAME="revisit-after" CONTENT="2 days">
eta name="description" content=" Sell your photos and make money"> <meta name="k
eta NAME="distribution" CONTENT="global">
eta NAME="resource-type" CONTENT="document">
eta NAME="rating" CONTENT="General">
eta NAME="ROBOTS" CONTENT="INDEX, ALL">
eta NAME="ROBOTS" CONTENT="INDEX, FOLLOW"> [if !IE]><!--> <html> <!--<![endif]-->

> “We will seek to provide some guidance on developing support systems to improve the transference of cyber risk learning to appropriate information asset handling.”

Chapter 13:
From learning to behaviour change

Chapter 13: From learning to behaviour change

Harvey Seale

> Most L&D professionals now know that it is the transference of learning into workplace behaviours that determines how effective a training course has been, not for L&D job security, but for the security and safety of the organisation.

Abstract

Most organisations try to combat the lack of cyber threat awareness with information security training, but the sad fact is that even if the training is compelling, if left at that, then only a small percentage of the desired behaviours will be transferred to the workplace.

Learning transference of any kind will not take place in an organisational vacuum. This chapter will seek to provide some guidance on developing support systems to improve the transference of cyber risk learning to appropriate information asset handling. This guidance should be considered in partnership with the strategic owners of organisational development and operational risk.

This chapter aims to:

- Know the impact and significance of learning transference within different internal risk cultures;
- Be able to identify the learning propensity of different types of risk culture;
- Help support a risk culture aligned learning response to support a cyber-risk management initiative.

Introduction

When Donald Kirkpatrick wrote the now world renowned research paper 'The Four Levels' in 1954, he was referring to the complacency of learning professionals satisfying themselves that effective training had taken place, by producing metrics such as the volume of training courses available, and the volume of employees that had been put through that training. Most L&D professionals now know that it is the transference of learning into workplace behaviours that determines how effective a training course has been, not for L&D job security, but for the security and safety of the organisation. This will not come as a surprise to most Chief Information Security Officers (Forrester, 2013), indeed the very fact that the activity known as 'Spear Phishing' (Lockheed Martin, 2012) has recently entered the cyber threat consciousness, underpins the fact that cyber criminals know that it doesn't matter how formidable information security policies and technological defences are, if there is an employee behind all of that security investment that is ignorant to the importance of information risk protocols, then there will always be a 'workaround' to organisational cyber defences.

> "Most organisations will place information security training at the centre of any plan to address Information Risk ignorance."
>
> *Donald Kirkpatrick, 1954*

Most organisations will place information security training at the centre of any plan to address information risk ignorance.

The 'lone gunman' theory of a breach coming from a disaffected employee is a threat, but assessing the likelihood of the risk of a breach materialising from that avenue, or from a loyal employee accidently leaving the cyber security door ajar, then most information security professionals would probably place the latter closer to the red area on the risk map.

Most organisations will place information security training at the centre of any plan to address information risk ignorance, however, in his 2002 book 'The Success Case Method' Brinkerhoff found that of any structured learning event only 15% of unsupported employees will successfully carry the desired new behaviours into the workplace, 70% try and fail with the final 15% not bothering in the first place. Accepting the research on face value it is reasonable to conclude that a little extra effort supporting employees, post learning, will lead to a lower likelihood of a breach as a result of ignorance.

After the learning event

This may seem to be an odd place to start in a chapter about cyber risk learning, but any seasoned Information Security Professional, adept in the specific cyber risk management protocols to protect the organisation, will have already included those requirements in a competent learning medium. Therefore this chapter is focused on supporting the learning transference from organisational risk requirement to workplace risk practice.

Risk architecture

A good place to start the support and monitoring of cyber risk learning is to have a look at the way in which risk information flows around the organisation (e.g. breach incidents, technical RCA findings, outcome and recommendations from cyber threat audits, etc.) and how IT contributes to, and interacts with, corporate operational risk information.In order to influence the organisation, and assess the effectiveness of cyber threat learning initiatives, there must be a collaborative forum external to day to day IT operations, comprised of influential business and IT risk stakeholders, in essence an Information Risk Committee. There will always be a need for the technical risk committee within IT and by structuring deference to the Information Risk Committee, this will bolster collaboration and business inclusion. Remember, business influence is an essential ingredient of any effectively embedded cyber risk awareness programme. Figure 13.1 depicts how this could look.

Risk culture

It is important to understand the type of risk environment within which you will be attempting to support the learning transference. The IRM has already conducted extensive research into the importance of risk culture, and how to go about understanding the risk culture in an organisation. Therefore there is no need to re-iterate that work here (see the bibliography for a reference to this research).

People 'feel' risks when they first come across them, in the case of a cyber risk this will typically be first encountered during the information security training.

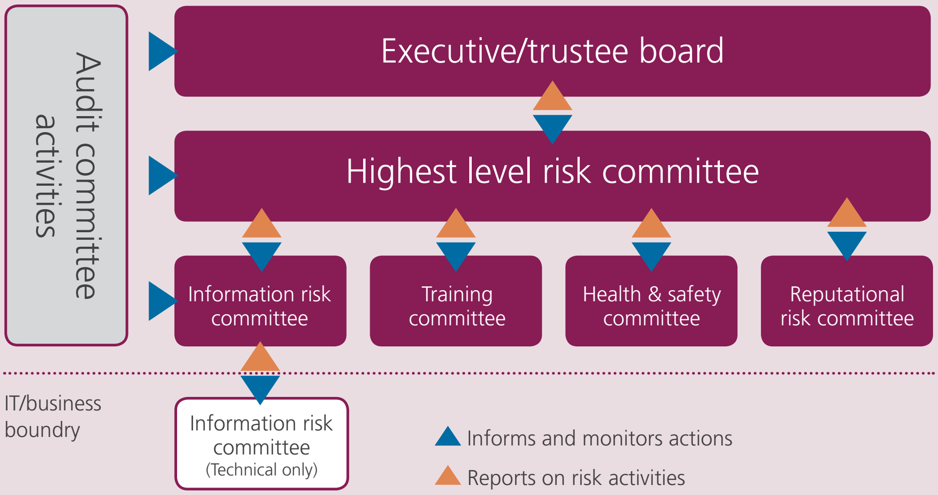
For the purposes of this chapter there will be an assumption that a risk cultural exercise has been conducted, or there is a sufficient understanding of the current risk culture to assess two key cultural components, risk perception and risk propensity. These cultural factors are believed to directly influence risk behaviour (Sitkin and Weingart, 1992), see figure 13.2.

People 'feel' risks when they first come across them, in the case of a cyber risk this will typically be first encountered during the information security training. It is this first feeling that will shape the employee perception to the inherent personal risk in a situation. It is only over time, with appropriately relevant information, cognitive thinking and rational discourse with respected peers will this feeling be 'shaped', and it is this component of individual risk learning that needs to be influenced during the process of learning transference.

Most people underestimate the impact or relevance of risk events that seem far off or unlikely, and most employees will take this perception, along with the associated risk behaviour, from the information security learning event on into workplace practice.

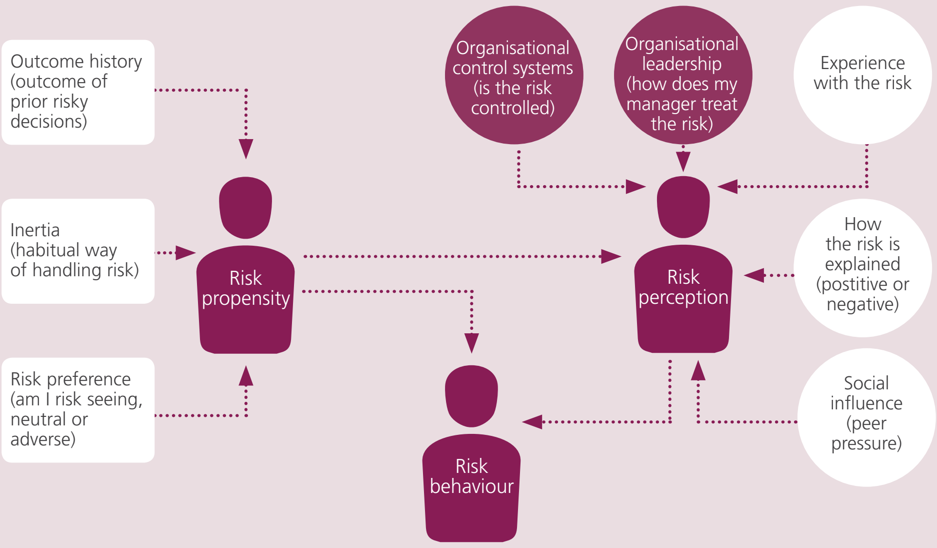
Clearly assessing and interpreting a risk culture is a nebulous and complex exercise, there are however easily obtainable indicators that will help support the learning transference process. With deference to Figure 13.2, the following cultural factors are among the most straightforward to determine and leverage:

Figure 13.1


Audit committee activities
Executive/trustee board
Highest level risk committee
Information risk committee
Training committee
Health & safety committee
Reputational risk committee
IT/business boundry
Information risk committee (Technical only)
Informs and monitors actions
Reports on risk activities

> Most people underestimate the impact or relevance of risk events that seem far off or unlikely.

Figure 13.2


Outcome history (outcome of prior risky decisions)
Inertia (habitual way of handling risk)
Risk preference (am I risk seeing, neutral or adverse)
Risk propensity
Organisational control systems (is the risk controlled)
Organisational leadership (how does my manager treat the risk)
Experience with the risk
How the risk is explained (postitive or negative)
Social influence (peer pressure)
Risk perception
Risk behaviour

1. **Outcome history and experience with cyber risk:** Has a senior influencer been the victim of, or significantly affected by, a cyber attack or the breach of an information asset? If so, approaching the individual to publicly sponsor (or even appear in) the information security learning programme, is likely to help motivate an employee to implement the desired information risk behaviours in the workplace, the greatest motivational effect will come from a personal experience;

2. **Risk preferences:** An understanding of this cultural factor, typically sourced through risk cultural questionnaires (see the IRM risk culture research paper for additional information), would provide a valuable insight into the spread (and concentration) of risk preferences, like all risk cultural data there are no hard facts, but table 13.1 provides some guidance and how this information could be leveraged to help support learning transference:

Risk Preference Type	Narrative	Factors to Consider	Importance of learning intervention in learning transference	
			Intervention Type	Impact
Risk Taking	Individual enjoys taking risks, is focused on achievement and the upside of risk rather than the negative impact of their risk behaviour.	In the learning event, be specific with the consequences of cutting corners for short term gains; i.e. The best time to assess the real benefit of a faster journey by running a red light is before an accident takes place.	Training at Induction: Refresher Training: Workplace Support:	High Low Med
Risk Neutral	Individual reacts to risks in line with statistical probability.	Without the benefit of experience, the negative impact of a cyber attack is only immediately apparent to information security professionals. Spend more time describing the personal impact rather than the technical cause, don't use jargon, and if you haven't done so already, get a senior stakeholder with a personal story to tell.	Training at Induction: Refresher Training: Workplace Support:	High Med Med
Risk Adverse	Individual will seek out activities that will have the smallest likelihood of causing harm or cost.	Same as Risk Neutral, and this is the best place to look for Cyber Risk Ambassadors.	Training at Induction: Refresher Training: Workplace Support:	High High High

> A job aid is a memory jogger designed to quickly provide the relevant information the employee need.

Supporting workplace transference

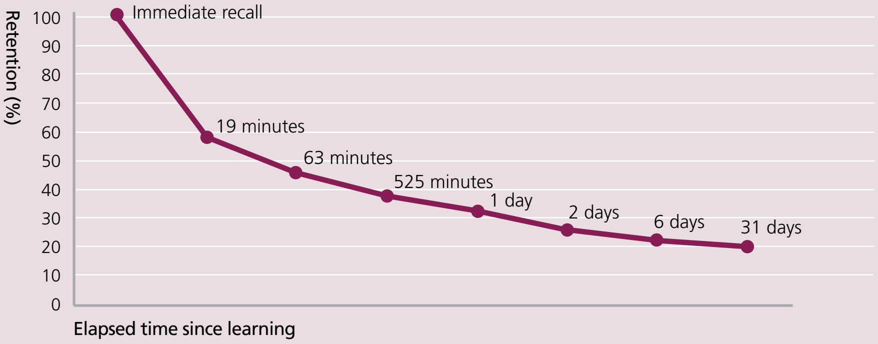
With deference to Brinkerhoff's work, Kirkpatrick identified numerous 'road blocks' to learning transference in the 70% of learners that 'tried and failed', the most common of which being learning retention. There are numerous tactics that can be deployed to address this, however, two of the simplest (and most cost effective) ways of supporting the learning are as follows.

Job aids

In essence a job aid is a memory jogger designed to quickly provide the relevant information the employee needs, job aids support two areas of learning transference:

1. They allow the training designers to focus the content on appropriate risk taking behaviour, the negative and personal impact of a breach and how the learning doesn't stop at the end of the course but continues on into the workplace. Without the support of job aids, consideration would need to be given to cramming in all the intense, and necessary, knowledge associated with correct procedure for all or most business activities, this naturally dilutes the overall impact of the learning event;
2. They allow the employee to walk out of the training with the broad concepts of the information security learning, safe in the knowledge that the detail of the required processes when protecting an information asset will be quickly accessible when they return to their desk. Naturally, most employees are not passionate about risk, cyber criminals and information security, so it is not surprising to learn that most employees will forget the facts and processes taught in an information security course. In fact employees may forget as much as 71% of the content by the following day (Ebbinghaus, 1850), see figure 13.3.

Figure 13.3: Elapsed time since learning



Remember the easier it is to access information security content, the lower the likelihood of someone giving up and performing the task in the best way they can remember.

Jobs aids broadly fall into two categories,

Contextual: This type of aid is just the right amount of information required to jog the memory for the task at hand. These will include notices above bins for secure disposal of information, a 'safe haven' check list near faxes, and popups on the first daily use of an internet browser.

Reference: For those employees that want to perform an activity, and understands that there is a specific way to do things, but cannot remember the exact process need a easily accessible place to get hold of this information, consider an intranet page or smart phone readable reference document where all of the learning content from the information security training is available, along with policies and procedures. Remember the easier it is to access information security content, the lower the likelihood of someone giving up and performing the task in the best way they can remember.

Refresher training

Most organisations do this, and the content may very well be the best that money can buy, however, if the refresher training is delivered in the same format, year in year out, then 'doing the information security course' will become a compliance overhead. A typical method to consider when keeping the content fresh draws on the risk information presented for consideration at organisational risk committee meetings. This will include legislative changes, new enforcement measures by regulators, the activities of hackers and internal emerging risks that may come from breaches or a risk control failure identified through audit (also known as a 'lessons learnt' or risk review process). In order to make the delivery more engaging consider having a pre-assessment, for year one onwards passing the employee in competent areas (most learning management systems can deliver this approach), therefore assuring the employee that the refresher training is targeted on their weak areas only, this is a technique that will carry more impact if it is combined with all other required compliance learning.

Monitoring effectiveness

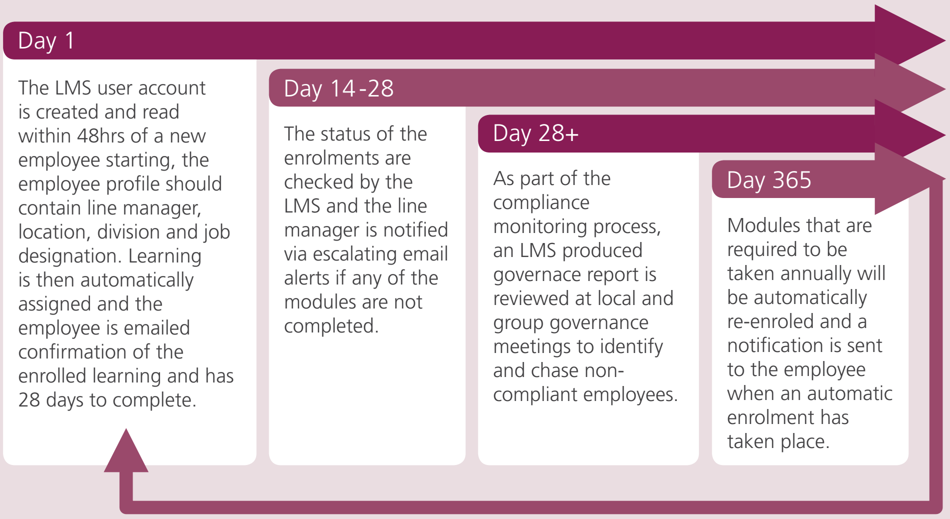
If an employee hasn't participated in the information security training in the first place, then they have little or no chance of applying the required behaviours in the workplace. Therefore, monitoring the effectiveness of learning transference starts with the attendance in the learning event. It is reasonable to assume that most organisations monitor this type of activity, but consider the scenario below to improve impact in this area.

Assuming for a moment that routine monitoring of attendance discovers that in the last 12 months 90% of employees have taken and passed the annual information security training, not bad, and in most organisations this would be classed as a green or satisfactory key performance indicator, however, how many organisations then put measures in to address the following questions:

1. When will the 'missing' 10% be exposed to the information security learning?
2. Are there employees within the 10% that have never been exposed to the learning?
3. Are there entire departments, teams or divisions within the 10%?

If the organisation has a learning management system (LMS), then a monitoring system similar to figure 13.5 could easily be developed in order to start collecting learning data to answer the above questions.

Figure 13.5



Day 1

The LMS user account is created and read within 48hrs of a new employee starting, the employee profile should contain line manager, location, division and job designation. Learning is then automatically assigned and the employee is emailed confirmation of the enrolled learning and has 28 days to complete.

Day 14-28

The status of the enrolments are checked by the LMS and the line manager is notified via escalating email alerts if any of the modules are not completed.

Day 28+

As part of the compliance monitoring process, an LMS produced governance report is reviewed at local and group governance meetings to identify and chase non-compliant employees.

Day 365

Modules that are required to be taken annually will be automatically re-enroled and a notification is sent to the employee when an automatic enrolment has taken place.

Look again at the current approach to cyber risk learning with the aim of bolstering the 'human firewall.'

In summation, this chapter seeks to invite the reader to look again at the current approach to cyber risk learning with the aim of bolstering the 'human firewall' against cyber attack. Suffice to say that a 90% learning penetration is a healthy metric, and it would be challenging to reach and sustain 100% compliance, but identifying the '10%' at the front of the learning initiative and understanding a little more about the human environment that learning is going to be applied in, will positively inform the delivery and monitoring assumptions of existing cyber risk learning strategy.

Whether that be the discovery that truculence, not absent mindedness, are the root cause of non-participation or something else, either way, understanding as much as possible about the existing cyber risk management ecosystem is just good governance.

Getting started

Try asking the following questions within your organisation

For HR and L&D

1. What initiatives are in place to support learners after the training event has taken place (e.g. reference library on the intranet, job aids, etc.) and how does information risk feature in these initiatives?
2. Do the post learning assessments gather data on what the employee has learnt, and how they are going apply the learning?
3. Is there a mechanism for employees to feedback on any difficulty they are experiencing in applying the learning?
4. Is there a process for monitoring employee attendance along with an evidenced process for the follow-up on non-attendees?
5. Does risk management and / or information security feature in the employee induction?
6. Are there current or future plans to assess the risk culture of the organisation?

For you, IT risk and operational risk

1. Does your organisation use a balanced score card where inappropriate information risk taking is measured?
2. Does the root cause analysis process, following a breach, include the extent human factors contributed to the incident, including environmental components such as poorly documented procedures or unnecessarily complex risk controls?
3. Does the information security training focus on securing the organisation or protecting the individual?
4. Is there a forum or committee where information risks are discussed in a jargon free manner? (see figure 13.1)

> Understanding as much as possible about the existing cyber risk management ecosystem is just good governance.

Bibliography

Brinkerhoff, Robert O. *The success case method find out quickly what's working and what's not*. San Francisco, CA: Berrett-Koehler, 2003. Print.

Hutchins, Eric. *"Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains."* Lockheed Martin (2010): Print.

Kirkpatrick, James D., and Wendy Kayser Kirkpatrick. *Training on trial how workplace learning must reinvent itself to remain relevant.* New York: American Management Association, 2010. Print.

Webster, Ruth, and David Hillson. *Managing group risk attitude.* Aldershot, England: Gower, 2008. Print.

Rose, Andrew. *"Reinvent Security Awareness to Engage the Human Firewall."* The S&R Practice Playbook. (2013): Print.

Multiple Authors. *"Risk Culture."* IRM (2012): 1. Print. Available from: **http://www.theirm.org/RiskCulture.html**

Smith, Keith. *The Affective Risk Management Organisation.* London: Taylor & Francis, 2011. Print.

Sitkin, Sim B., and Amy Pablo. *Reconceptualising the determinants of risk behavior.* Austin: Dept. of Management [University of Texas at Austin], 1991. Print.

Kahneman, Daniel, Paul Slovic, and Amos Tversky. *Judgment under uncertainty: heuristics and biases.* Cambridge: Cambridge University Press, 1982. Print.

> “The costs and expenses of data breaches which result in the wrongful disclosure of personally identifiable information can be wide ranging.”

Chapter 14: Information security and privacy risk transfer – insurance solutions

Chapter 14: Information security and privacy risk transfer – insurance solutions

Tim Stapleton

Organisations run the risk of either being crippled by attacks against their networks or losing valuable proprietary information which can result in extensive first party losses.

Introduction

The costs and expenses of data breaches which result in the wrongful disclosure of personally identifiable information can be wide ranging. According to the 2013 Annual Study: Global Cost of a Data Breach conducted by the Ponemon Institute, the average cost of a data breach to an organisation in 2013 out of the countries surveyed ranged from $1.1 million (India) to $5.4 million (US). Similarly, organisations run the risk of either being crippled by attacks against their networks or losing valuable proprietary information which can result in extensive first party losses. Although each scenario has its own set of unique factors, the costs and expenses incurred by the victim organisations remain fairly consistent. Since the early 2000's, the insurance industry has offered specific risk transfer solutions to help offset the financial impact to companies that can result from the ever growing litany of information security and privacy threats they face.

You have in previous chapters been presented with an analysis of costs and expenses that are largely uninsurable. This chapter examines financial elements that may be transferred to a dedicated security & privacy or "cyber" insurance policy that result not only from data breaches, but also from failure to comply with the provisions contained in dynamic privacy legislation.

Insurable Loss

Data breaches can occur in a number of ways including attacks to companies' networks from malicious code, viruses, or less exotic offline issues such as lost laptops or other portable devices, loss of physical documents, or simply forgetting to shred documents before disposing of them. Regardless of how it happens, an organisation must take certain steps once it becomes aware that personally identifiable information may have been compromised. As a matter of best practice, those steps typically include consulting with legal counsel, conducting a forensics investigation, notifying and providing remediation services to potentially affected individuals, consulting with a public relations firm, and establishing a call centre to field questions. Similarly, companies must take certain steps if cyber attacks result in network down time or loss or corruption of their valuable digital assets.

Since the vast majority of companies are not set up to engage in these actions on their own (nor is it advisable to do so), they must engage with third parties. While these actions generate additional costs, many studies have shown they can be the difference between restoring the trust of customers and permanently damaging a company's reputation.

A forensics investigation determines the severity and scope of a breach involving compromised computer systems or networks.

The insurance industry has in the past 10-15 years developed products that cover many of the specific costs and expenses that can result from a data breach or privacy incident and which typically fall outside the scope of traditional Property & Casualty insurance policies like General Liability, Property, and Professional Liability. In the following section, we will further analyse specific costs and expenses associated with information security and privacy incidents that can typically be transferred to a dedicated insurance policy including:

1. Forensics Investigation
2. Notification of third parties
3. Call Centre Administration
4. Fraud Remediation Services
5. Public Relations
6. Legal Advice, Defence, & Settlement
7. Regulatory Proceedings, Fines, & Penalties
8. Business Income Loss
9. Restoration of Electronic or Digital Assets
10. Cyber Extortion Costs and Expenses

Forensics Investigation

A forensics investigation determines the severity and scope of a breach involving compromised computer systems or networks. It is considered a crucial step in the post breach response process since it helps victim companies accurately assess the situation before going public. Time and time again, companies that act too quickly to publicly disclose details of a data breach may actually worsen the situation and suffer additional long-term costs. The costs are also higher than average even in situations where companies are simply complying with local laws and regulations that compel notification within short timeframes. According to the same Ponemon 2013 Annual Study: Global Cost of a Data Breach companies that notify quickly ended up paying up to $37 more per record compared to the average by companies that took the appropriate time to analyse the event. In addition, there have also been cases in which breached companies that skipped a forensic exam mistakenly notified unaffected customers.

A forensics exam can be performed either by a company's internal staff or an outsourced third party. However, internal investigations can inadvertently lead to destroyed evidence or questionable authentication, so third parties are typically engaged to ensure quality and maintain objectivity. This is particularly important in the context if third party lawsuits and regulatory investigations that might take place after the event. Companies are generally in a more defensible position having engaged an objective third party.

The costs of a forensics exam may vary greatly, but generally, firms charge on a fee basis with average fees ranging from $200 up to $1000 per hour and in some cases, more. Fees can be impacted depending on the company's jurisdiction, the complexity of the breach, whether it occurred at the companies site, a vendor location, or in the cloud, the skill level and number of forensic investigators required, travel expenses, how well prepared the company was prior to the incident, and whether the incident is still ongoing throughout the investigation just to name a few. The investigation process can take days, weeks, or even months in some cases to fully determine the scope of the problem since investigators must conduct interviews with employees in addition to looking at purely technical elements.

The cost of engaging a third party forensics firm is typically covered under most network risk policies.

Notification of Third Parties

A number of global jurisdictions have enacted privacy legislation that include some form of data breach notification provisions. These provisions require companies or individuals that maintain unique personally identifiable information of individuals to notify those individuals if such information is lost, stolen or otherwise compromised. Regardless of the legal requirement, many companies believe it is good business practice to notify affected individuals in the event of a breach since it serves to effectively mitigate long term reputational damage.

Fees can be impacted depending on the company's jurisdiction, the complexity of the breach, whether it occurred at the companies site, a vendor location, or in the cloud, the skill level and number of forensic investigators required, travel expenses, how well prepared the company was prior to the incident, and whether the incident is still ongoing throughout the investigation just to name a few.

In the European Union, legislation has been proposed that would update the current comprehensive EU Data Protection Directive by changing it to a regulation. In addition to greater uniformity and centralized enforcement, the proposed regulation includes a data breach notification provision which imposes a broad requirement to provide notification if personal information of EU citizens is compromised. The proposed penalties for non-compliance are severe and could be quantified by assessing up to 2% of the company's global annual turnover. The proposed changes are being considered for adoption in 2014 with expected enforcement beginning in 2016.

In the US, forty-six states, the District of Columbia, Puerto Rico and the Virgin Islands have enacted data breach notification laws. The state laws require companies or individuals that maintain unique personally identifiable information of individuals to notify those individuals if such information is lost, stolen or otherwise compromised.

While the basic purpose of each state notification law is similar, differences arise in the specific process required such as the use of U.S. Postal Service, certified mail, or other special delivery. A breached company will need to review each state's specific requirements, which is a time consuming and costly process on its own. Many companies hire third party law firms or consultants to assist in determining applicability of state notification laws after a breach has occurred.

Additionally, Massachusetts and other states have adopted "compliance" models that allow for less stringent reporting requirements when specific security measures such as encryption are in place at the time of the breach. One of the goals behind this approach is to encourage companies to take proactive steps to protect personal information.

Countries in other regions such as Mexico, the United Arab Emirates (Dubai International Financial Centre), Japan, and New Zealand have all passed notification laws so this issue is clearly on the radar of politicians and lawmakers all over the globe. While the impact of notification laws is not intended to be punitive towards companies that hold sensitive personal data, the end result is a guarantee that a company will incur additional expenses if they lose such information.

Notification costs can vary depending on the number of records or individuals affected. A scaled approach is common with the charge per notice gradually decreasing as the number of records or individuals increases. Costs can range from $.50 to $5 per notice. The cost can be impacted by whether the customer database has been kept up to date with current contact information and where the individuals are located around the globe. Address validation and establishment of secondary contacts will also increase the overall cost. Average notification costs based on the Ponemon Global report ranged from $22,232 in India to as much as $565,020 in the US.

The direct legal expenses associated with determining applicability of local notification laws and general costs of notifying potentially affected third parties are typically covered under most security & privacy insurance policies. The costs associated with implementing proactive risk management procedures to mitigate the impact of a breach before it occurs, however, are not.

Call Centre Administration

Many companies consider it best practice to include a phone number in the notification letters that recipients can contact to obtain more information about the extent of the breach, the company's response, and the steps they should take. Based on the 2013 Cyber Risk Claims study conducted by NetDiligence, the average number of records compromised in breaches fielded by participating insurance carriers was 115,000. There were other outliers not included that reached into the tens of millions of records so it is important to consider the potential for wide ranging severity and scope. Given those figures, it is reasonable to assume that many companies do not have the internal administrative capacity to handle a significant increase in the volume of calls they might receive after a breach. Companies, therefore, often hire third party vendors that specialize in comprehensive breach response to establish call centres that are staffed by individuals armed with scripts to field questions and concerns. Costs are typically calculated by call volume, number of weeks or months the centre will be operational, as well as hours available (24/7 versus normal business hours). The cost of establishing a call centre is also a general staple of coverage under most security & privacy insurance policies.

Fraud Remediation Services

Personal information is increasingly being used to commit identity theft so it is important that companies recognize the need to provide free fraud remediation services to potentially affected customers.

While credit or identity monitoring is not required by most notification laws, many companies believe that providing such services maintains good customer relationships and can often be the difference between running a clean post breach campaign and drawing the ire of both customers and regulatory authorities. Consequently, credit and identity monitoring along with other fraud remediation services have become standard elements of a comprehensive beach response. The practice is also backed up by the findings of a study titled "Empirical Analysis of Data Breach Litigation" conducted by Carnegie Melon University and Temple University which suggests that "the odds of a firm being sued are 3.5 times greater when individuals suffer financial harm, but 6 times lower when the firm provides free credit monitoring."

"the odds of a firm being sued are 3.5 times greater when individuals suffer financial harm, but 6 times lower when the firm provides free credit monitoring."

While credit monitoring services are focused primarily on financial elements like credit history and account activity, services such as identity monitoring go further by tracking activities relative to medical, employment, and other types of fraud. One service may be more appropriate than the other depending on the type of information compromised during a breach along with the global jurisdiction in which it occurred and where the affected individuals reside.

Generally, the number of potentially affected individuals that take advantage of such services when offered is very low. However, research suggests that the need for these services is increasing. A 2013 Identity Fraud Report conducted by Javelin Strategy & Research found that "1 in 4 data breach notification recipients became a victim of identity fraud in 2012, compared to less than 1 in 5 in 2011." The report also suggests that while credit card information may be the most popular target of attacks, other elements of personally identifiable information may be more useful for committing fraud.

Combined costs for credit monitoring, identity monitoring, and restoration can generally range from $10 to $35 per individual per year. The costs can add up very quickly when you consider that one breach can compromise thousands or even millions of records. Such costs are generally covered under most security & privacy policies.

Public Relations

In addition to the actions already mentioned, companies may engage an external public relations firm that specializes in damage control to help mitigate harm to its reputation caused by a data breach. The direct cost of obtaining a PR firm is covered under most security & privacy policies, however the indirect adverse impact on the company is more difficult to insure. According to the 2013 Ponemon Global Study, lost business costs can account for a significant amount of overall costs to the organisation. At the lowest end of the scale, companies from India experienced an average of $283,341 in lost business while US companies experienced an average of $3,030,814 in lost business. While the amounts of lost business resulting from the breach are generally not covered by most insurance policies, the direct expenses incurred to notify, provide credit/identity monitoring, and wage a public relations campaign are covered and can have a direct impact on reducing the amount attributable to lost business.

According to the 2013 NetDiligence Cyber Claims Report, the total average cost of all crisis services in a data breach amounted to USD $364,000. Direct costs of consulting with a public relations firm typically range from $200-$500 per hour. Other costs associated with the process might include advertising through print, television, or other media, all of which are generally insurable.

The average cost for legal defence was $258,000

Legal advice, defence and settlement

Claims from a data breach can come from a number of parties, but most frequently from affected consumers and financial institutions. Defending these claims results in legal defence expenses in addition to the actual cost of settlements or indemnity payments. According to the 2013 NetDiligence Cyber Liability and Data Breach Insurance Claims Study, 6 legal damages represented the single largest component of costs paid by insurance carriers who participated in the survey. The average cost for legal defence was $258,000 while the average legal settlement was $88,000 which is significantly down from the prior year study's figure of $2.1 million.

Regardless of whether identity theft actually takes place, consumers whose personally identifiable information has been compromised as a result of a breach may file suits alleging a number of violations including:

- Negligence
- Breach of warranty
- Failure to protect data
- Failure to disclose defects in products or services regarding capabilities of protecting data
- Unreasonable delay in remedying suspension of service or loss of data
- Violations of various applicable state/ federal laws
- False advertising
- Unfair or deceptive trade practices

Consumer claims are typically filed as class actions in the US and tend to have limited success given the difficulty in proving injury in the absence of actual identity theft. However, new legal theories continue to evolve and so may the outcome of such claims. While it is uncertain whether consumers may successfully prove damages, it is certain that the breached company will face significant costs in hiring legal counsel to defend itself. While class actions are most prevalent in the US, the legal theories around proving actual damages may certainly pave the way for individual claims in other global jurisdictions.

As you can see from the following Advisen Market Insights graphs (Figures 14.1 and 14.2), litigation from cyber and data breaches has steadily increased since 2005 with most activity taking place in the US.

In addition to claims made by consumers, banks that issue payment cards have also sought damages from breached companies for the costs of reissuing compromised cards. It is estimated that a bank may pay between $12 and $22 to reissue a single payment card.7 The cost of card reissuance is one of the reasons banks have been successful in recouping this expense from retailers or other breached organisations.

> Claims from a data breach can come from a number of parties, but most frequently from affected consumers and financial institutions.

Issues can also occur relative to a company's service offering. An organisation with business customers may experience errors and omissions (E&O) claims that allege negligence in professional services following a data breach. For example, consider an IT service provider that needs to disable key security functionality for several hours during a network upgrade performed for a third party.

Figure 14.1: Cyber Litigation Frequency Index

The Cyber Litigation Frequency Index represents a measure of the frequency with which lawsuits accompany cyber events in the Advisen Master Significant Actions and Cases (MSCAd) database. To create the Index, Advisen analyzed the frequency of cyber occurrences within a defined group of cyber case types and matched accompanying lawsuits based on data as of February, 2013. The ratio of the number of events with accompanying lawsuits compared to the overall count of events as of 2005 is represented by 100. Subsequent years were then compared against the baseline of 100.

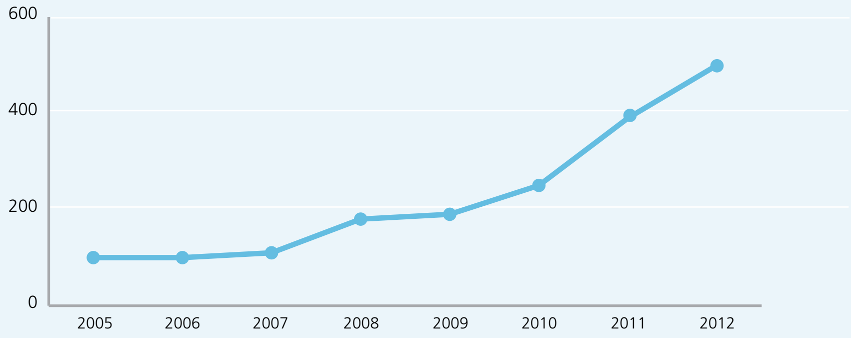
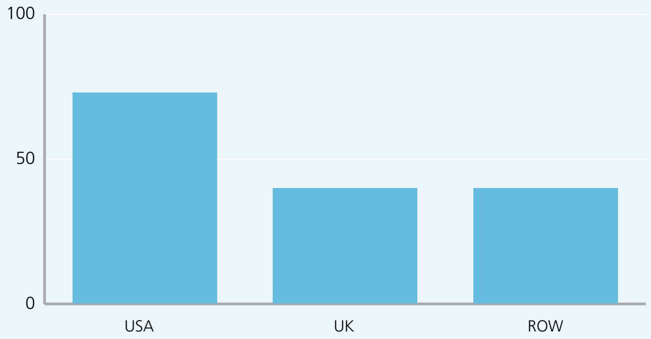


Figure 14.1: Global Relative Litigation Index

The Global Relative Litigation Index provides an indication of the frequency with which lawsuits accompany cyber events in the US compared to the UK and the Rest of the World. To create the indices, Advisen compared the consolidated eight year (2005 to 2012) count of lawsuits and divided by the count of events for the US, the UK and the remainder of the world. The UK and other countries are compared to the US baseline frequency of 100.



Increased scrutiny by law making bodies and enforcement agencies around the globe is affecting all companies.

During that installation, an attacker could gain entry to the network and download a cache of personally identifiable information from company's customer database. The customer may pursue legal action against the service provider alleging negligence in technology professional services that lead to the breach, and seek damages for costs incurred including notification, credit monitoring of third parties, forensics, and other expenses.

Finally, derivative suits may also be filed by shareholders alleging that Directors and Officers didn't abide by their fiduciary duty to protect customer data. This illustrates the point that data breaches are not an IT risk but a business risk and should be discussed with the board of directors as they may be held directly accountable. Standard D&O policies may not cover 1st or 3rd party costs arising from wrongful disclosure of data even if a director or officer didn't perform their fiduciary duty to protect the organisation's intangible assets.

Looking at this issue in the liability context is particularly important due to the average costs that victims may incur if actual identity theft takes place after a breach since those expenses may well be used to effectively quantify damages. Depending on the nature of information compromised, there may also be allegations of emotional distress which can drive up costs and influence the company's decision to settle.

Regulatory proceedings, fines and penalties

Increased scrutiny by law making bodies and enforcement agencies around the globe is affecting all companies. In some jurisdictions that have adopted comprehensive privacy or data protection legislation, the laws apply to all industry sectors while other territories like the US have adopted a more sectoral approach that focuses on specific industries like health care and financial services firms due to the sensitive and personal nature of the information they handle. In many cases, enforcement agencies have the ability to investigate companies not only if there is a data breach, but also if there is reason to believe the company has not generally complied with the applicable legislation. Regardless of what triggers the investigation, the company must hire legal counsel and defend itself. It may also be subject to fines and penalties depending on whether local laws and regulations dictate.

One example of a Federal law is the Privacy Rule under the Health Insurance Portability and Accountability Act of 1996 (HIPPA), which outlines basic requirements for healthcare organisations regarding the handling of Protected Health Information. As part of the American Recovery and Reinvestment Act of 2009 (ARRA), the Health Information Technology for Economic and Clinical Health Act (HITECH) established a tiered civil penalty structure for HIPAA violations. Fines can range from $100 per violation to a maximum of $1.5 million. The Department of Health and Human Services has already fined several entities as a result of violations of the Privacy Rule.

The ICO is empowered to issue fines of up to £500,000 to organisations in breach of data protection laws which are frequently broken within cyber security events.

After a breach, transparency will typically foster good will between the company and the regulator. However, the costs of an investigation remain significant given the need for specialized counsel and the cost of potential fines or penalties. Fines and penalties may or may not be insurable depending on jurisdiction and the actions of the company.

In the UK the Information Commissioners Office (ICO) is empowered to issue fines of up to £500,000 to organisations in breach of data protection laws which are frequently broken within cyber security events. Since it was given the powers to issue Civil Monetary Penalties in April 2010, the ICO has issued over £4.6m of fines against organisations.

The range in financial penalties varies significantly across the globe with some countries / jurisdictions yet to apply a structure of fines, to the courts ascertaining the costs of damages right through to the fines awarded by the Brazil and Mexico authorities of over US$1.5m (€1.155m).

Case Study – Brighton and Sussex NHS Trust

The trust was fined £325,000 – the largest fine by the ICO to date – for sensitive patient data being found on hard drives sold on eBay.

The trust was unsure how the drives could have been removed from the premises but admitted that the drives may not have been secured at all hours during which a contractor had access.

In general, many of the Western governments have well established legislation and high penalties of several hundred thousand dollars.

In addition to government regulatory bodies, there are also non-government entities that set best practice standards and set contractual fines and penalties for non-compliance. One such entity is the Payment Card Industry Security Standards Council that was established by the major payment card brands in 2006. The Council established the Payment Card Industry Data Security Standard as a uniform best practice requirement for any company that processes, stores or transmits credit card information. The Council engages third party vendors to assess compliance levels of organisations subject to the standard. Non-compliance can result in fines or penalties. Fines can range from $5,000 to $100,000 per month.

The sophistication and scope of modern cyber attacks can easily cripple a company's network which in turn can prevent the flow of commerce and in some cases, result in the loss of income.

Business income loss & dependent business income loss

The sophistication and scope of modern cyber attacks can easily cripple a company's network which in turn can prevent the flow of commerce and in some cases, result in the loss of income. For example, an entity that conducts most of its business online with no physical storefront locations is at great risk of business income loss if a security event such as a virus, malicious code, or distributed denial of service attack brings their website or network down for a period of time. Many traditional insurance policies are designed to cover business income loss if it results from a physical peril such as a storm, fire, wind, flood, etc… However, coverage may not apply if the BI loss is caused by a network security event. Traditional policies that do provide coverage typically do so in a limited capacity with a narrow coverage trigger and a small sub-limit.

Many dedicated security & privacy policies contain an element of first party loss designed to cover net income before taxes an organisation incurs during the measurable period in which they are unable to generate revenue after a network security incident or cyber attack takes place. Some policies are also triggered by administrative errors or general system failure independent of a cyber attack. Dedicated coverage solutions also typically include a provision for extra expenses the company incurs to minimize, avoid or reduce the measurable outage.

Also of great value is a provision in many dedicated policies that will pay for "dependent business income loss" or essentially, the downstream BI loss a company incurs due to a network outage caused by a cyber attack or security incident aimed at a service provider on which the company relies to maintain their network. Those traditional policies that provide any level of coverage for this scenario typically do so to an even more limited extent than direct BI loss.

Restoration of electronic or digital assets

Many companies operate on the assumption that workers will have access to critical data. The rise in use of new technologies like cloud computing and mobile devices means that companies now have the ability to collect, store, access, maintain, and share more data than ever before. In order to harness these new technologies, data must be converted to electronic or digital format. This mass movement towards digitisation acts as a double edged sword in that it creates unprecedented efficiencies and enables progress while at the same time makes companies more susceptible to the perils of cyber attacks than ever before.

As the cyber threat environment has evolved, so too have the methods of "cyber extortionists".

Customer lists, databases, project specifications, blue prints, financial, competitive, private or confidential information that is maintained by a company in electronic or digital format are considered highly valued intangible assets that if altered, destroyed, corrupted, stolen, or otherwise compromised as a result of a cyber attack or other security incident, will result in significant first party expenses to restore or recollect. Dedicated security & privacy insurance policies typically pay out for the expenses to first determine whether the data can be restored or recollected. If it can be restored or recollected, insurance policies may pay for additional costs to actually restore the data to its original form. While the intrinsic value of intellectual property is not covered by security & privacy policies, the fact that direct costs are included may provide some cushion to mitigate the impact of the incident.

Incidents resulting in the loss, corruption or alteration of digital assets represent only a small fraction of the overall claims submitted to insurance carriers offering dedicated security & privacy policies so there is limited actual loss data from which we can draw a firm conclusion on the average costs, however, there are several benchmarks that act as guideposts. The post incident process is very similar to other types of security and cyber events in that it may require the expertise of an outside forensics investigation firm to fully realize the scope and severity of the incident. Companies may also incur costs in implementing internal disaster recovery plans.

Cyber extortion expenses

As the cyber threat environment has evolved, so too have the methods of "cyber extortionists". Threats from individuals purporting to steal valuable information from a company unless they are paid a sum of money still exist, however, cyber extortionists are becoming more and more sophisticated in their methods. "Old school" types of threats have given way to malware referred to as "ransomware" that often freezes a victim's computer or takes it hostage unless the end user pays a sum of money to the extortionist. Another type of malware referred to as "scareware" baits the end user into clicking on a link that appears to be from a legitimate security firm by first creating the false perception that a virus exists on their machine and needs to be removed.

These types of incidents tend to be small scale for the time being, however, the use of new technologies to carry them out will only serve to increase the frequency of attacks. According to a recent press release, the FBI's Internet Crime Complaint Center (IC3) received 289,874 complaints, averaging more than 24,000 complaints per month in 2012. It is clear from the numbers that companies must be prepared to deal with the financial impact which can manifest itself in the form of forensics investigations and actual payments to perpetrators.

Cyber insurance is seen as a growth market with over 30 carriers offering capacity.

Conclusion and recommendations

Many of the issues discussed above may be contemplated by security & privacy or "cyber" insurance policies. Carriers understand that claims are inevitable but to help mitigate catastrophic losses, many underwriters have taken a risk management approach for this coverage rather than just plain risk transfer. Carriers typically offer robust propositions that include proactive risk assessment and risk management advisory services as well as access to experienced data breach service providers. This is great news for a risk manager at an organisation who can partner with their carrier to address elements beyond just financial loss.

Cyber insurance is seen as a growth market with over 30 carriers offering capacity. A risk management approach allows underwriters to display cyber insurance as a partnership with the insured to help reduce risk with certain loss control methodologies. While buyers may have an increasingly hard time assessing risks and avoiding big losses, risk management innovations from insurers, brokers and partners may help make a difference.

With the evolution of the threat, litigation and regulatory landscapes, it is only reasonable to expect that cyber policies will evolve at an equal pace. Since 2003, we have already seen an impressive evolution of the coverage grants carriers are willing to provide and that have now become market standard. Companies are now in a unique position to take advantage of this growing area.

Risk manager tools

Risk transfer is typically the final step in the process of evaluating your company's risks and exposures. Beginning a discussion with your Chief Financial Officer or Board of Directors can be challenging if they have had limited exposure to the topic of information security and privacy. The following is a list of basic questions to ask both personnel within your organisation and your insurance broker to begin the discussion around whether it is appropriate to transfer security and privacy risk:

- What types of personal or sensitive information does my company collect?
- What is my company's global footprint? What is the global footprint of my company's customer base?
- What privacy and data security laws and regulations might my company be subject to based on the responses above? How aggressive are the regulatory enforcement agencies in those jurisdictions?
- Based on my industry, service offering/operations, and customer base, what are my biggest exposures – first party or third party?
- How many critical business functions do I outsource to third parties?
- How much private and sensitive information do I share with third parties?
- Do my contracts contain indemnity and hold harmless provisions in my favour in case my vendor suffers a data breach or security incident that has a negative impact on me?

- What is my company's mobile device usage policy? Is BYOD enabled and encouraged?
- Where, under existing traditional Property & Casualty insurance policies, might I have coverage for the financial loss elements covered in this chapter?
- Do I have an incident response plan that includes "post breach" vendors who will provide crisis management services on short notice such as forensics investigation, notifications, fraud remediation, public relations, legal advice, etc…?

Sources:

Advisen Cyber Liability Insurance Market Presentation, Jim Blinn, Cyber Liabilities Insurance Conference, London, February, 2013

Empirical Analysis of Data Breach Litigation

Sasha Romanosky, David Hoffman, Alessandro Acquisti, Carnegie Melon University, Temple University

NetDiligence Cyber Risk Claims 2013 Study, Mark Greisiger

Symantec/Ponemon Institute 2013 Cost of a Data Breach: Global Analysis

Practical Law Company Multi-Jurisdictional Guide 2012/13, Data Protection

Digital Transactions "Mass Reissuance May be Overkill in Merchant Breach Cases"

www.digitaltransactions.net/index.php/news/story/1274

Javelin Strategy & Research, 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters

IC3 2012 Internet Crime Report Released: **http://www.fbi.gov/news/pressrel/press-releases/ic3-2012-internet-crime-report-released**

Data Breach Cost: Risk Costs and Mitigation Strategies for Data Breaches, Tim Stapleton, CIPP/US

Hit Ratios are Still Very Low for Security & Privacy: What are companies waiting for? Neeraj Sahni and Tim Stapleton, CIPP/US

> “This chapter explores the areas in which investment may be required to deliver an effective information security programme.”

Chapter 15: Investing in cyber security

Chapter 15: Investing in cyber security

Matt Hillyer

Introduction

As both the risk and regulatory pressures around cyber security continue to increase more and more organisations have or will begin to look at investing in comprehensive information security programmes. For some organisations the current perceived impact of an information loss is less than the potential cost of investment but as the chapter titled 'Iceberg impact of a loss' demonstrates the true cost of an incident is ever growing when organisations consider the indirect as well as direct costs of an incident. Indeed the upward trend in regulation particularly the EU Data Privacy Regulation and the proposed EU Cyber Security Directive will dramatically change the penalties for getting it wrong.

This chapter explores the areas in which investment may be required to deliver an effective information security programme and considers some of the additional business benefits which may be realised on top of the risk mitigation. The chapter will review investment against three headings:

- People
- Process
- Technology

People

The investment in training and awareness sessions for your people can be a very effective way to mitigate a number of cyber and other information security risks. This element of an information security programme can also provide good evidence of effective controls should an employee's actions lead to a cyber breach.

IT can only provide part of the solution.

Some of the training options available include:

Training Type	Outline Costs
In House Training Course	In general an in-house programme takes around 3 to 4 weeks to write followed by a further 3 days for any refresh of content for future courses. In addition there will be the costs of taking people out of the business for the day and any travel or facility costs.
External Training Course	Accredited Cyber Risk courses are now available and cost around £1,500 for a 3 day course
E-learning package	As a guide an e-learning package costs around £3,000 – £5,000 per 20 minutes of content dependent upon the level of customised graphics and interaction required. Similar costs would be required for updating the material
Communications Campaign	Communications programmes can vary hugely in costs but as a rough figure to fulfil a training brochure to a 10,000 employee business would cost around £3,500. Costs will rise if promotional posters and other collateral are required

Training Type	Pros	Cons
In House Training Course	• Tailored to your specific business needs • Low cost to replicate once it is developed	• Time and resource consuming to develop • Ongoing requirement to refresh the content and keep it up to date
External Training Course	• Expert content, always up to date and leading edge • No setup time required	• Costly if required for a large employee base – more suited to specialist roles • Not necessarily aligned to business requirements
E-learning package	• Can be easily deployed to remote workers • Able to test understanding with interactive quizzes	• Only suitable for limited amounts of content per session to maintain user interest
Communications Campaign	• Relatively easy to reach a large audience at low cost • Variety of support media available to reinforce messages	• Push only messaging which may not be understood or acted upon • Needs to be supplemented by additional training to embed learning

"Having implemented suitable training programmes can be seen as mitigation should an information security breach occur. In the ICO Data Protection Regulatory Action Policy, they state that regulatory action may not be taken where there has been a "non-compliance with the data protection principles, but where the Data Controller has taken reasonable steps in the circumstances to prevent a breach."

This approach is certainly good practice and given that employees are seen as one of the biggest risks of information security breaches it will have a major impact on your risk exposure.

The effectiveness of any training will be influenced by both the risk culture within the organisation and both the timing and follow up process for the training itself. This is explored in more detail in the chapter – Cyber Risk Learning to Behaviour.

Process

Enhancing existing business processes and adopting new ones can also address a number of cyber risks. With any investment it is about knowing which areas will make the most difference to your organisation. The Department of Defence within the Australian Government set out 4 processes which they state could prevent 85% of targeted cyber intrusions within the Defence Signals Directorate:

- Use application whitelisting to help prevent malicious software and other unapproved programs from running
- Patch applications such as PDF readers, Microsoft Office, Java, Flash Player and web browsers
- Patch operating system vulnerabilities
- Minimise the number of users with administrative privileges.

These relatively simple recommendations provide focus for organisations of all sizes, but particularly SMEs, in addressing process improvements.

Other areas of investment associated with processes include:

- Governance – The systematic approach and framework which supports the management of cyber risks within your organisation
- Information Systems Incident Response – The processes and procedures for documenting and responding to a cyber loss
- Business Continuity Incident and Crisis Management – The ongoing management and stakeholder communication following a cyber loss
- Business Continuity Planning and Testing – The development of business continuity documentation and
- Controls Testing – The regular and systematic testing of the information security controls in place
- Third Party Compliance – The adherence of suppliers to the information security standards required by your business.

> “100% security is expensive, intrusive and rarely achievable in the fast paced world we live in.”

Technology

Technology can be both an effective and costly way to tackle cyber risk and creating a compelling argument for why you should invest in a particular system or piece of software is key. Most likely, as with both People and Process related investments, you will not be able to invest in everything. As stated in the introduction to this Cyber research, “100% security is expensive, intrusive and rarely achievable in the fast paced world we live in”. Therefore, getting the balance right of investing in technology to prevent cyber losses and in technology to respond to incidents when they happen is very important. Typical areas of technology investment include:

- Logical Access – The controls around authorisation and authentication on information systems
- Data Loss Prevention – The systems used to identify and prevent the unauthorised loss of data from systems
- Logging and Monitoring – The technology used to capture and trend access data to identify possible breaches
- Penetration Testing – The testing of IT security through the simulation of external attacks
- Security Architecture – The IT systems capabilities to protect information within it.

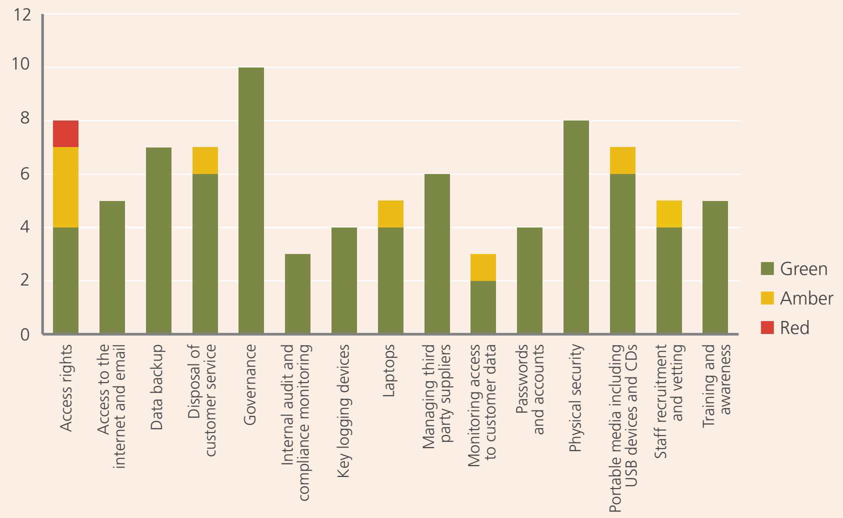
Prioritising Investment

Having a clear understanding of current weaknesses or awareness of gaps against certain quality standards can help focus an organisation on where to prioritise investment. The following approaches are examples of how you could graphically represent current performance.

The first approach is taken from the Good Practice Guide issued by the former FSA, now the FCA. Section 4 of the guide lists examples of the good and poor examples of data security and by extrapolating the good practices, organisations can evaluate their level of good practice knowing these have already been baselined within the financial services industry. By assessing on a predetermined scale and utilising a RAG status approach to identify performance gaps against the guide, organisations can see where to focus their attention which in this case, is on access management and one control of laptops. In the example chart on page 228, five levels of compliance were used as shown in the table above the chart:

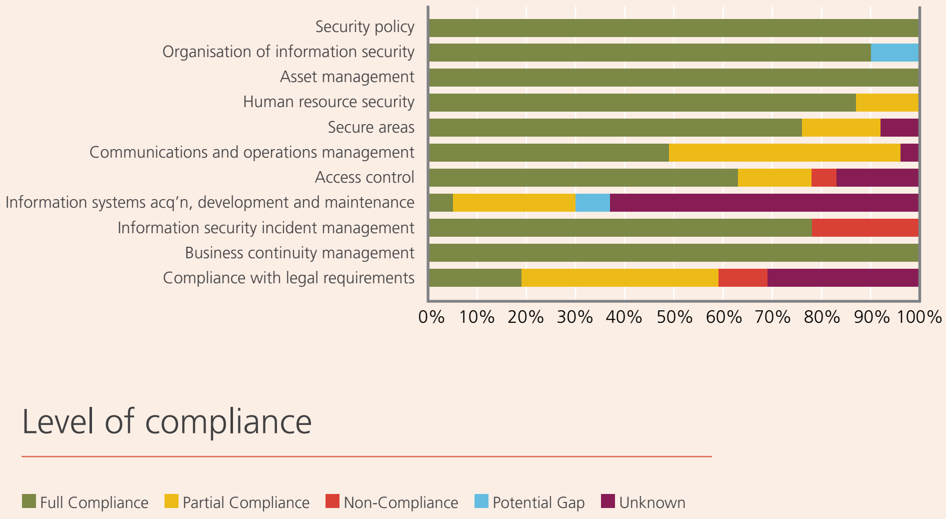
Rating	Definition	RAG Status
Achieved	All components of the requirement set in the FCA guide are operating effectively	Green
Good Practice	Most of the components of the requirement set in the FCA guide are operating effectively but there are some low risk design or operating issues to be resolved	Amber
Needs Improvement	The is no or little adherence to the components of the requirement set in the FCA guide and they represent a risk to the organisation that requires remediation action	Red
Unknown	The level of adherence of the requirement set in the FCA guide is unknown and requires further investigation	Amber
Accepted gap	The requirement specified in the FCA guide either does not apply or the organisation has formally accepted the risk(s) arising from non-adherence	Green

FCA Good Practice Guide



For those that use the ISO 27001 or aspire to, determining levels on compliance against ISO 27001 is also possible in graph form and in this case it also has some additional controls for the FCA Good Practice Guide shown opposite. In this instance, the originator of the assessment clearly has some further research on the "unknown" areas but has some clear non-compliance in incident management, access control and compliance with legal requirements whilst potential gaps exist in two other areas but need to be validated.

ISO Compliance Per Section



One thing we can be sure of is the impact of a cyber loss is increasing.

Developing the business case

Having reviewed all the areas of possible investment, you now get to the 'million dollar' question – "How do you get the board to provide the capital required?" This is not an easy question to answer and ultimately as with any business case it is an amount demonstrating a suitable return on investment (ROI). This chapter does not attempt to numerically demonstrate the ROI of the case for cyber investment but detailed below are some areas which can help describe the financial benefits of a successful cyber security programme:

Opportunity benefits:

1. Improved availability of investment – a strong reputation for information security will be more attractive to potential investors
2. Accreditation to International Standards – achieving a required standard can improve competitive advantage and customer perception
3. Development of effective recovery plans – any incident will be contained and managed to ensure that lost operational time and ultimately financial losses are kept to a minimum.

Avoided downside benefits:

1. Prevented/reduced fines – A successful programme can reduce the likelihood of fineable losses but in the event of an incident evidence of a clear, board supported programme can reduce regulatory fines.
2. Protection of Intellectual Property – The theft of critical designs and other IP could have devastating results for organisations particularly small and medium sized enterprises.

One thing we can be sure of is the impact of a cyber loss is increasing and the likelihood of an event is increasing so the ROI calculation is increasingly supporting the investment case for a cyber security programme.

Conclusions and recommendations

As seen within this chapter, an all-encompassing information security programme can require significant investment in a number of areas. Often though this level of investment is not available and it is therefore vital as a risk professional to advise the business on the most important areas to prioritise.

> A successful information security programme can bring Internal transparency on cyber risks and the controls in place.

A successful information security programme can bring a number of benefits to your organisation:

- Greater organisational awareness of cyber risk and its potential impact on the business
- Internal transparency on cyber risks and the controls in place
- Clear compliance with external regulatory controls
- Demonstrate strong business practices to investors
- Improved business performance
- Competitive advantage through a stronger customer value proposition.

Reading list and websites

1. **http://www.itgovernance.co.uk/shop/p-1408-managing-cyber-security-risk-training-course.aspx**
2. ICO, *Data Protection Regulatory Action Policy – version 2.0,* August 2013
3. FSA, *Data Security in the Financial Services*, April 2008 accessed via **http://fca.org.uk/firms/being-regulated/meeting-your-obligations/firm-guides/information-gathering/data-security**
4. **http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm**

Questions for the board
1 Which areas associated with cyber risk is it mandatory for the organisation to invest in?
2 What are the information ‘crown jewels’ which the organisation must protect
3 What will the business impact be from losing this information?
4 How much would it cost a 3rd party to obtain this information and what could it be worth to them?
5 What are your customers’ expectations of your cyber security programme?

> “
> In recognition of the seriousness of the threat the GCHQ is supporting a number of initiatives and schemes to help protect information systems in the UK and build the necessary cyber capability within the workforce.“

Chapter 16: Cyber risk management – how do I know I have the right people?

Chapter 16: Cyber risk management – how do I know I have the right people?

GCHQ

Cyber-attacks were listed as a Tier 1 threat to our national security, alongside international terrorism.

Cyberspace continues to revolutionise how many of us live and work. Alongside the huge business and social benefits of 24 hour global connectivity comes a host of risks to the availability, integrity and security of the information we hold. The seriousness of the threat posed is recognised by the UK government in its 2011 National Security Strategy. Cyber-attacks were listed as a Tier 1 threat to our national security, alongside international terrorism.

In recognition of the seriousness of the threat and the huge opportunities of a digitally connected world, the Government Communications Headquarters (GCHQ) is supporting a number of initiatives and schemes to help protect information systems in the UK and build the necessary cyber capability within the workforce. GCHQ's work forms part of the National Cyber Security Program (NCSP) which is a cross government strategy involving key players such as the department for Business Innovation and Skills (BIS), Cabinet Office and the Engineering and Physical Sciences Research Council (EPSRC).

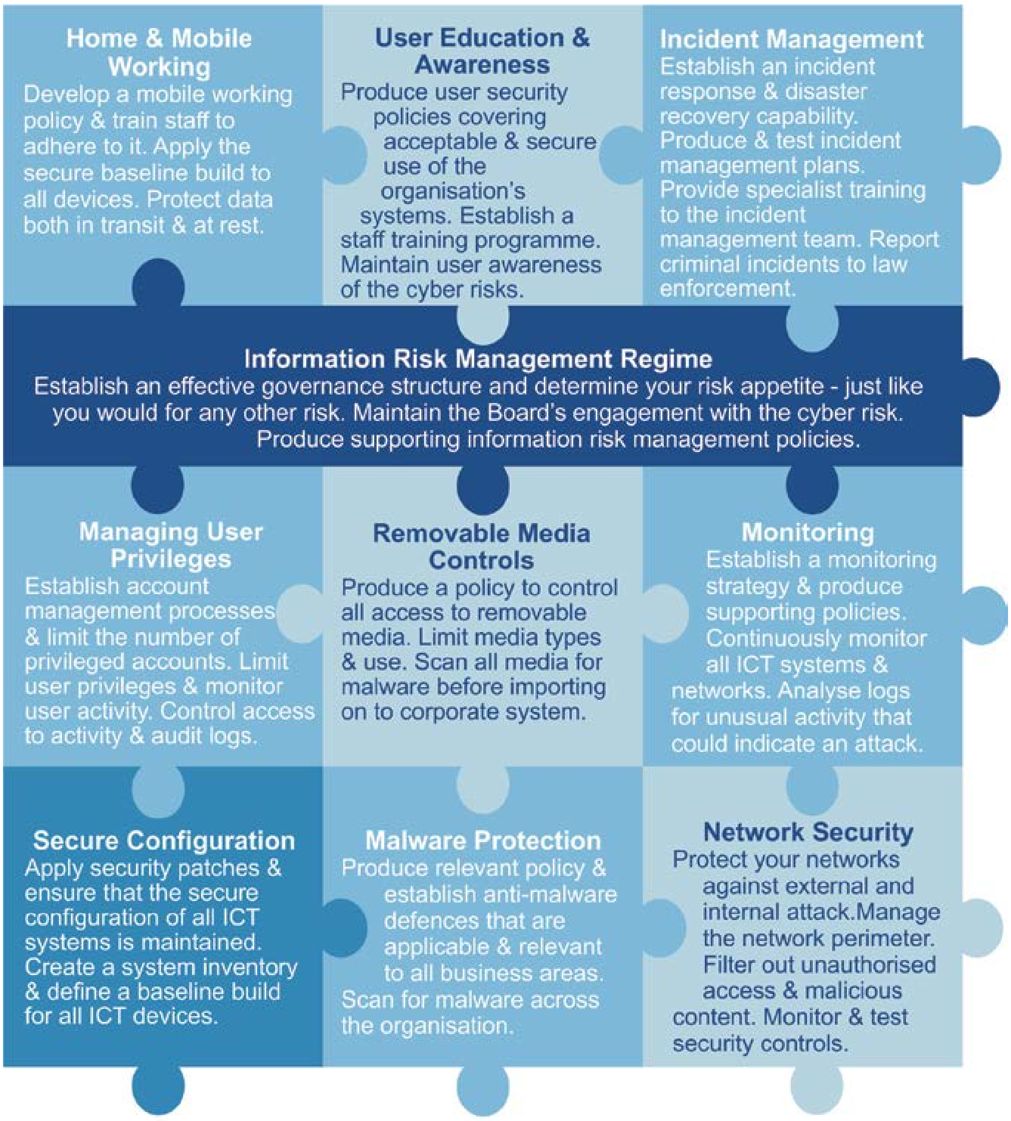
A critical step in the strategy is to help place responsibility for cyber security at board level. Happily, this doesn't require board members to have a deep technical knowledge but it does require them to acknowledge that risks to information should be treated in the same way as financial or business risks, especially as threats and vulnerabilities are constantly changing. Through CESG, the information security arm of GCHQ, and working with BIS and the Centre for the Protection of National Infrastructure (CPNI), a high level guide outlining the ten steps to cyber security was published in 2012, illustrated in Figure 16.1. Whilst it is not an exhaustive guide, it does set out clear, practical steps which senior executives should direct to be taken to improve the protection of networks and the information they carry.

The National Security Strategy also recognised the nascent rise of cyber threat has left a global shortage of individuals with the appropriate skills, knowledge and experience to mitigate it. As a developed country, rich in cutting edge research, design, financial services and intellectual property, the UK has been a persistent target for cyber criminals and sophisticated attacks. Whilst GCHQ has traditionally concentrated on HMG information systems, it is now working as part of a cross government initiative to bring academia and industry together to grow the skills base and improve the cyber security of UK plc, to more effectively and efficiently mitigate the cyber risk.

There are a number of key programmes in place to achieve this:

> A critical step in the strategy is to help place responsibility for cyber security at board level.

Figure 16.1: Ten Steps to Cyber Security



Home & Mobile Working
Develop a mobile working policy & train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit & at rest.

User Education & Awareness
Produce user security policies covering acceptable & secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Incident Management
Establish an incident response & disaster recovery capability. Produce & test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Information Risk Management Regime
Establish an effective governance structure and determine your risk appetite - just like you would for any other risk. Maintain the Board's engagement with the cyber risk. Produce supporting information risk management policies.

Managing User Privileges
Establish account management processes & limit the number of privileged accounts. Limit user privileges & monitor user activity. Control access to activity & audit logs.

Removable Media Controls
Produce a policy to control all access to removable media. Limit media types & use. Scan all media for malware before importing on to corporate system.

Monitoring
Establish a monitoring strategy & produce supporting policies. Continuously monitor all ICT systems & networks. Analyse logs for unusual activity that could indicate an attack.

Secure Configuration
Apply security patches & ensure that the secure configuration of all ICT systems is maintained. Create a system inventory & define a baseline build for all ICT devices.

Malware Protection
Produce relevant policy & establish anti-malware defences that are applicable & relevant to all business areas. Scan for malware across the organisation.

Network Security
Protect your networks against external and internal attack.Manage the network perimeter. Filter out unauthorised access & malicious content. Monitor & test security controls.

CCP is an important step in creating a unified standard for those working in the UK Cyber Security industry.

CESG Certified Professional (CPP)

Launched in October 2012 the scheme consists of a number of cyber security roles which are assessed at three levels of competence. Having been successfully deployed across government, CCP is now available to Cyber Security professionals working in the private sector. Not all the current roles will have a direct correlation to the private sector but as the scheme develops, additional roles will be added.

CCP is an important step in creating a rigorous, unified standard for those working in the UK Cyber Security industry. By extension it gives companies a level of assurance in the competence of their employees and contractors.

The scheme is run by three independent certification bodies which have been appointed and are audited by CESG for consistency and quality. They are:

1. APM Group.
2. IISP, CREST and Royal Holloway ISG consortium.
3. BCS, the Chartered Institute for IT.

For details on the scheme please visit:

www.cesg.gov.uk/awarenesstraining/IA-Certification/Pages/index.aspx

GCHQ, BIS and EPSRC working with Academia

GCHQ and EPSRC have recognised 11 UK universities as having an established cyber security research pedigree based on their academic excellence, impact and scale of activity and research in areas that underpin cyber security. These Centres of Excellence enhance the UK's cyber knowledge base through original research and make it easier for potential users of research to identify the best cyber security research that the UK has to offer.

In addition, GCHQ has agreed to sponsor 12 doctoral studentships in cyber security research in 2013-14 with a further 11 scheduled to start in 2014-15.

Collaboration between EPSRC, BIS and GCHQ has seen the establishment of two Research Institutes in cyber security, which is developing capability in strategically important topics. A third is in the process of being set up and led by CPNI. Research Institutes are virtual collaborations of selected universities which will allow academics from different scientific disciplines including social scientists, mathematicians and computer scientists to work together to carry out research on our toughest cyber security challenges.

GCHQ is also developing a process to accredit MSc courses in cyber security to make it easier for prospective candidates and employers to recognise those MSc courses which are seen as meeting a good standard – this is planned to go live in autumn 2014. Masters in cyber security subjects provide a number of benefits including a bridge between STEM degrees and cyber security specialisms, and are also a great way for people in mid-career to 'top-up' their knowledge or move into cyber security as a change of career path.

For more information on GCHQ Academic schemes please visit:

http://www.cesg.gov.uk/awarenesstraining/academia/Pages/index.aspx

Summary

These initiatives are just a snapshot of the work GCHQ is involved in alongside its partners in government, industry and academia "to build the UK's cross-cutting knowledge, skills and capability to underpin all other cyber security objectives by extending knowledge and enhancing skills". By setting standards for cyber security professionals; developing and supporting the talent of the future; and creating the right environment for cutting edge research in cyber security, GCHQ is acting as a catalyst for change.

> By setting standards for cyber security professionals; developing and supporting the talent of the future; and creating the right environment for cutting edge research in cyber security, GCHQ is acting as a catalyst for change.

case WM_COMMAND:
{MessageBeep(MB_OK);}
else EndDialog(hwnd,1);
(n=0;n<gButtonNum;n++) adiArr[n]=adiT[n],adiArr[n].Enab=adiArr[n].Enab && adiArr[n].Cor;
case ID_CANCEL:
EndDialog(hwnd,0);
return 0;
ShowWindow(hWnd,SW_MAXIMI
SetForegroundWindow(hWnd);

> “As the cyber environment evolves, risk management and internal audit will need to keep pace.”

Chapter 17:
Auditing cyber risks

Chapter 17: Auditing cyber risks

David Canham

Internal auditors will need to ensure that they have the appropriate knowledge about cyber risk.

Introduction

A critical component of all risk governance is gaining assurance, through internal audit, that the risk management processes in place are working correctly and that resources are being deployed effectively. As the cyber environment evolves, risk management and internal audit will need to keep pace. Cyber risks, in their broadest sense, should be reflected, following a risk-based assessment, in internal audit planning and execution. Internal auditors will need to ensure that they have the appropriate knowledge about cyber risk and internal audit and risk management and operational management should work closely together to share intelligence and validate control responses.

We consider in this chapter some of the key considerations for the internal audit of cyber risk.

1.1 Principles of internal audit

The global Institute of Internal Auditors (IIA) defines internal auditing as "... an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes"[17]. The internal audit function provides assurance to management teams, non-executive directors and audit committees on the health of the control environment, reporting back where issues are discovered and identifying where additional action is needed.

The 'three lines of defence' model (endorsed in the UK by the IIA and the Institute of Directors) sets out a simple framework for understanding the various levels of control and assurance:

- **1st Line** – operational management controls deployed by day to day line management as part of managing the business. For example, in the cyber risk context there may be a team of control testers in the Chief Information Officer's department giving assurance that feeds into both operational governance and also the organisation's audit plan.
- **2nd Line** – monitoring and facilitation of operational management by the risk management team or others such as the compliance function. The 2nd line provides advice, education, challenge and oversight to 1st line activities. As part of this 2nd line role, assurance teams work with the 1st line to assess weaknesses and vulnerabilities in the control environment and compliance with legal and regulatory frameworks, using the organisation's regulatory environment and inherent risk register to direct activity.

[17] http://www.theiia.org/guidance/standards-and-guidance/ippf/definition-of-internal-auditing/

> In a large organisation the complexity and legacy infrastructure issues will lead to difficult decisions on where best to deploy internal audit resources.

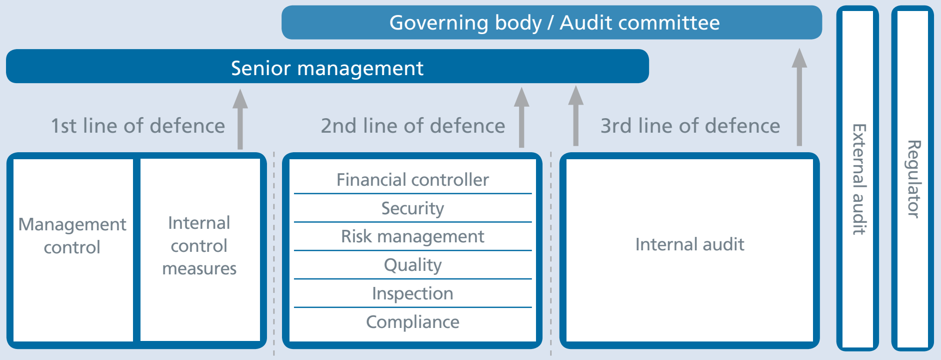
- **3rd Line** – the internal audit function, providing assurance on how the first and second lines of defence are working by conducting independent reviews on a risk based basis.

This model is represented diagrammatically in Figure 17.1. This diagram is taken from the IIA publication "What Every Director Should Know About Internal Audit" which contains further useful information and which can be accessed here: **http://www.iia.org.uk/media/481822/what_every_director_should_know_4-4-13_web_version.pdf**.

Traditional audit activity is planned using inputs from previous audits, a review of the organisation's risk register, a view on external trends and cyclical reviews on core processes. Reviews are carried out using a combination of interviews and testing of controls, the results are analysed and reported and action plans developed based on a severity rating. External audit partners will also provide additional assurance and may also conduct "deep dive" reviews of certain areas.

Clearly not everything can be audited all the time – how limited resources should be allocated is a key factor. In a large organisation the complexity and legacy infrastructure issues will lead to difficult decisions on where best to deploy internal audit resources. In an SME audit, resource may need to be shared or procured through a contract and ensuring that this is deployed to the most appropriate risks is essential to achieving maximum value. In either case a thorough assessment of the risk profile provides a framework for these decisions to be made and will stand the test of external scrutiny with regulators if there was to be an incident. The organisation can legitimately argue that it was adequately managing the risks and prioritising audit tasks based upon the risks.

Figure 17.1: Three Lines of Defence Audit Model



In setting the audit plan a number of sources need to be consulted to ensure the most comprehensive plan possible.

This chapter will now examine the traditional approach to auditing and suggest how in a "cyber" environment the role of the internal auditor may differ.

The traditional auditing approach

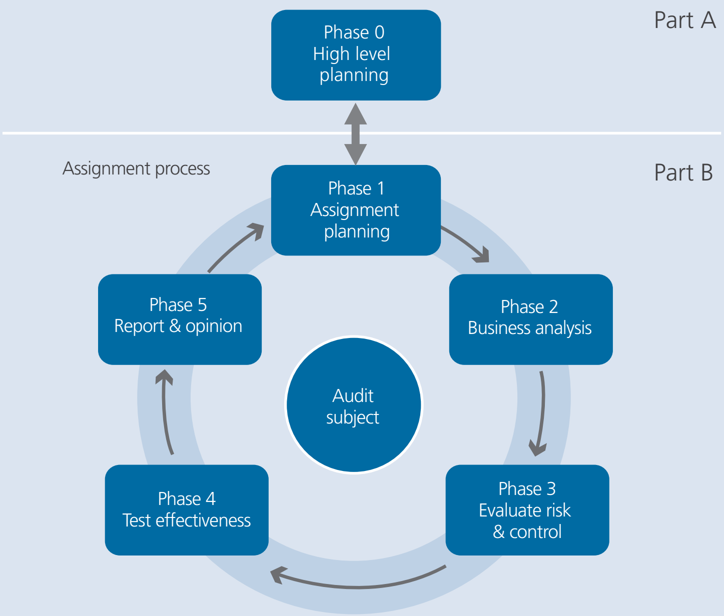
There are a number of variations on the internal audit approach but the basic high level characteristics are the same as set out in figure 17.2 below:

Phase 0 – high level planning

In setting the audit plan a number of sources need to be consulted to ensure the most comprehensive plan possible. These sources include but are not limited to:

- Inherent risk profile
- Current company risk universe
- Group / organisational standards
- Previous audits
- External sources
- Regulatory considerations
- Management / audit committee direction
- 1st / 2nd line assurance programme

Figure 17.2: A high level overview of audit planning


Part A
Phase 0 High level planning
Part B
Assignment process
Phase 1 Assignment planning
Phase 2 Business analysis
Phase 3 Evaluate risk & control
Phase 4 Test effectiveness
Phase 5 Report & opinion
Audit subject

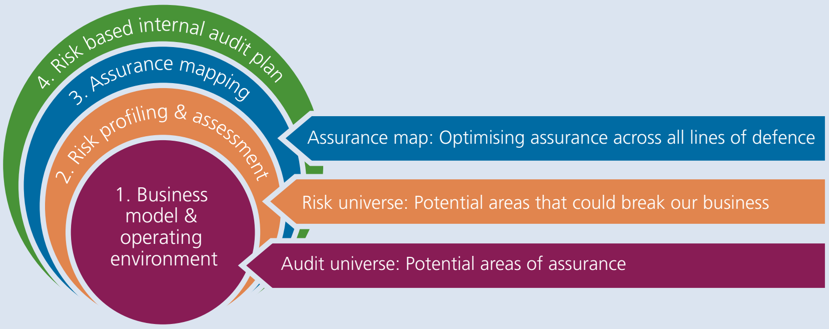
> In the modern organisation there will be a network of internal and external parties that will impact and influence the audit plan.

> Most extended enterprise networks have varying degrees of openness towards their suppliers.

Traditionally based around an annual plan, internal audit teams are now adopting a more flexible approach based around rolling plans on a "three plus nine" or "six plus six" basis. Detailed guidance on risk based audit planning can be found on the Institute of Internal Auditors website **www.iia.org.uk** based around models such as the four step model for financial services outlined below in figure 17.3.

In the modern organisation there will be a network of internal and external parties that will impact and influence the audit plan. For instance specific contract terms may be required to allow the organisation to review processes involving suppliers and outsourcers. Utilising standards such as ISAE3402 (a global assurance standard for reporting on controls in service organisations) may provide comfort. Regulators may also direct an audit of certain activities should an organisation be censured. Most extended enterprise networks have varying degrees of openness towards their suppliers. As cloud provision increases (see chapter 7) some providers have been reluctant to let customer organisations' internal audit teams in to challenge and assess against their own control environment. Whilst it is understandable that cloud providers might want to avoid being inundated by customer inspection regimes, this clearly presents a problem for the internal auditor who can find themselves reliant on vendor standard third party assurance assessments or limited data obtained from remote access to a vendor. This is an issue that the internal auditors need to identify early on. Ideally they should influence the contractual wording for such service provisions otherwise they could find their role undermined at the point of audit two or three years into the contract.

Figure 17.3: Risk based audit in financial services


4. Risk based internal audit plan
3. Assurance mapping
2. Risk profiling & assessment
1. Business model & operating environment
Assurance map: Optimising assurance across all lines of defence
Risk universe: Potential areas that could break our business
Audit universe: Potential areas of assurance

Source: IIA

For evolving cyber threats a different way of thinking may be required.

Phase 1 – assignment planning

Once the plan has been created individual audit assignments can take place. Terms of reference should be produced, in conjunction with the front line management, outlining the scope of the internal audit activity and taking into account:

- the key stakeholders that need to be engaged
- an estimate of the time required, and
- an assessment of the risks and controls which will form the basis of the audit activity.

Phase 2 – business analysis

As the review begins and internal auditors arrive on site, the first activity undertaken is business analysis.
This process is important to establish a common view of the process environment to be reviewed. This can take the form of review of process manuals, the creation of process flow charts and / or narrative describing how processes that are subject to audit operate and will be reviewed. In addition a control register of the points of key controls should be created, firstly as part of identification process and secondly to enable effective testing and alignment to the risks being reviewed.

Phase 3 – risk and control analysis

The second stage of the on site process is the analysis of the organisational risk register. This will link the controls identified in the business analysis phase to the risk register and also identify any areas where gaps exist in the risk register. The internal auditor will typically build a risk and control matrix from this information which will inform testing and help in the formulation of findings which will be logged as the review progresses and help inform the final reporting.

Phase 4 – test effectiveness

Once the risk and control matrix is in place and the processes mapped and understood, testing can take place utilising a mix of 1-2-1 interviews, technical testing via 3rd parties e.g. firewalls, PCI DSS compliance and reviews of 3rd party controls through interaction with suppliers. The findings of this process and issues identified will ultimately lead to the final audit report.

Phase 5 – report and opinion

The final stage is the production of the audit report. The findings are graded on an organisational risk materiality hierarchy. There is usually an expectation that management will remediate in line with this rating. A higher rating usually dictates a need for a more speedy resolution plan. The aggregated view of all audits in a specific control area will form an "audit opinion" which is reported periodically to the board, audit committee and, if relevant, external interested parties.

It makes sense to follow a set pattern to ensure quality and integrity of the organisational audit plan but the traditional process takes time and is set alongside the control environment of the organisation concerned. With a fast paced cyber environment a traditional approach may be sufficient for data security controls but for evolving cyber threats a different way of thinking may be required.

> The scope of the planning phase of the audit programme must consider the expanded cyber threat landscape.

Applying Audit Approach to the Cyber Environment

So when applying the traditional approach to the "cyber environment" there are a number of considerations including and not limited to:

High level planning

The scope of the planning phase of the audit programme must consider the expanded cyber threat landscape. Traditionally audit plans have been built around the organisational process map and risk register but in a "cyber" environment additional external factors need to be considered, as described elsewhere in this document, for example:

- Increasingly, as found in the IRM SIG's research there will be a network of suppliers, 3rd parties and advisors across the organisation. There are a number of ways of assuring compliance and control through accredited standards but the internal auditor needs to decide if this satisfies the level of assurance the parent organisation requires to meet its own risk tolerance.
- Organisations need to have sufficient monitoring mechanisms in place to give proactive warning of cyber intrusion. Traditional controls around security such as policies, procedures, firewalls etc. are subject to internal audit scrutiny but increasingly the internal auditor also needs to consider the wider requirement for more proactive and enterprise-wide monitoring and scanning. For example does the organisation have a security operations centre?
- External intelligence is increasingly important in planning and assessing the risks within an organisation. With a reluctance to report and share information on breaches in the private sector particularly, reviewing of publically available information in planning, utilising informal links between companies and reviewing industry databases such as ORIC (in the insurance sector) can assist making the organisational audit plan more comprehensive.

Control and remediation

Throughout the research for this document, the authors have highlighted control areas and practical advice across the organisational cyber landscape. From an audit viewpoint the threat landscape is extensive, from internal to external, financial to franchise, criminal to disruptive. Essentially when creating the test plans and the risk and control matrix the internal auditor needs to consider not just the controls in place but the mix of controls. At a high level the internal auditor should consider the following control types:

- **Preventative** – controls designed to prevent a specific event from occurring or a risk crystallising such as segregation of duties. Data loss prevention (DLP) solutions are becoming more common place and questions should be raised where these do not exist or are inconsistent across a larger enterprise. Malware protection needs to be up to date and in line with the more sophisticated attacks seen across many industries. Another preventative control may be the auto-patching processes to reduce the likelihood of zero-day attacks.

Traditional periods of six month programmes are unlikely to be adequate to address a cyber threat that changes and evolves on a daily basis.

- **Detective** – controls that are designed to provide an early warning of a problem or detect a risk crystallising such as IT estate monitoring. From a cyber viewpoint the internal auditor needs to consider more targeted controls looking at individual databases where the organisation's "crown jewels" data is held, rather than general event monitoring across the organisation. Clearly, this gives the internal auditor some important questions to raise about data classification within the organisation and the ability to interpret and understand where data is in motion and at rest. Once again, DLP can help here to detect if the right data is in the right place.
- **Corrective** – controls that are designed to fix events or risks should they crystallise, such as business continuity plans. In the cyber context corrective controls can be key and need to be deployed immediately should an organisation, regardless of size, find itself under attack. Processes such as the organisation's "Emergency Fix" process should be examined; the RACI[18] of who needs to make decisions and who has the ability to enact may be an area for the internal auditor to explore.

In addition the time periods for remediation need to be considered in the context of the threats identified. Traditional periods of six month programmes are unlikely to be adequate to address a cyber threat that changes and evolves on a daily basis.

Despite this there has to be a degree of pragmatism. For instance, a large organisation with considerable legacy IT and an aged desktop estate will take longer to address a threat than an SME. An example could be the movement from XP to Windows 7. In an organisation that is global and has multi-locations within the same jurisdiction, management of transition from one to the other requires more complex planning than for a smaller enterprise. Further, the larger organisation may also uncover applications that cannot be migrated or will become unstable and these may require the internal auditor and the process owners to take a different approach when considering control and remediation. It may even result in accepting a risk to the business rather than destroying multi-million dollars of business, but the decision needs to be a conscious one.

Traditionally, internal auditors need to be strong in their engagement with management to ensure a sufficiently speedy reaction to emerging risks, control breakdowns and failures identified but also cognisant of the wider organisational issues and the constraints these provide.

Organisations should ensure that their internal audit teams have the appropriate qualifications and skills to meet the demands of this new and changing risk environment.

[18] A responsibility assignment model defining roles and identifying who is "Responsible, Accountable, Consulted or Informed."

> As the "cyber" environment evolves so does the need for risk management and internal audit to keep pace.

> Early stage input into contractual terms may be needed to ensure that assurance can be obtained.

Pace of audit

With a fast paced threat landscape surrounding the "cyber" environment the traditional approach to auditing has to be questioned. There is clearly a place for the traditional based control testing around the organisation's information control environment but there is also the consideration of what role does internal audit play in the investigation of an incident. Organisations have established processes for dealing with the immediate aftermath of a "cyber event" but the forensic investigation into the weaknesses leading up to the event and the impacts could benefit from independent oversight.

Conclusions and recommendations

As the "cyber" environment evolves so does the need for risk management and internal audit to keep pace. Our recommendations are as follows:

- Cyber risks, in their broadest sense and including, for example, social media risks, are likely to be a significant future risk area for most organisations and this should be reflected, following a risk-based assessment, in internal audit planning and execution.
- Particular attention should be paid to the risks associated with interaction and data exchange with suppliers (including cloud services) and other third parties within the extended enterprise. Early stage input into contractual terms may be needed to ensure that assurance can be obtained.
- Close attention should also be given to the behavioural aspects of cyber risk – the actions and motivations of individuals – as well as the technical and process aspects of information security.
- Internal auditors must keep their knowledge of cyber risks up to date to be able to provide assurance in respect of their management. This should cover both pro-active and reactive controls and the use of external intelligence.
- Internal audit, risk management and operational management should work closely together to share information about cyber risks. The internal auditor should not be seen as the 'headmaster marking homework' but as an integrated part of the risk management process working with the 1st and 2nd line assurance functions to share intelligence and validate control responses.
- The independence brought by internal audit should be a valuable part of the investigation process after an incident or as a response to unusual patterns of activity picked up in monitoring.

Reading list and websites

1. *Institute of Internal Auditors accessed* December 2013 via **http://www.theiia.org/guidance/standards-and-guidance/ippf/definition-of-internal-auditing/?search%C2%BCdefinition**
2. *Institute of Internal Auditors accessed* December 2013 via **http://www.iia.org.uk/media/481822/what_every_director_should_know_4-4-13_web_version.pdf**

“As a not-for-profit organisation support is invaluable in helping us maximise our investment in the development and delivery of world class risk management education and professional development.”

IRM

T: +44(0) 20 7709 9808
E: enquries@theirm.org
W: www.theirm.org

Address:
Institute of Risk
Management
6 Lloyd’s Avenue
London
EC3N 3AX
United Kingdom

CGI

Paul Hopkins
Cyber Security
Technical Authority
paul.hopkins@cgi.com

Wendy Holt
Strategy &
Innovation Director
wendy.holt@cgi.com

£150