

IRM Charities Special Interest Group

Technology and cyber security: Tackling the risks

www.theirm.org/charities

irm

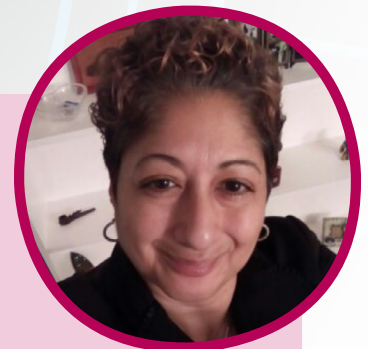
Developing risk professionals

Prepare for risk in the digital age with the Institute of Risk Management's new

Digital Risk Management Certificate

The essential qualification for tomorrow's risk practitioner

"I have chosen the digital risk course due to the evolving digital landscape. Cyber-crime is on the rise and, therefore, effective management to mitigate cyber risk is paramount. Poorly managed risks from the outset, could cause devastating consequences to the stability of the financial market. With the evolution of blockchain other cyber risks will inevitably arise. Preventative methodologies, measures and strategies will also need to be considered."



Tracey Simmons
Senior Business Analyst
Bermuda

This qualification covers

- > The digital world and the "4th industrial revolution"
- > Digital disruption, organisational and societal change
- > Risk management principles and practices in relation to digital risk
- > Ethical implications of digital innovation
- > Principles and practice of cyber security and incident management
- > Audit and assurance for digital and emerging risk

Enrolments now open

- > Members: £1095
- > Non-members: £1195

Produced in collaboration with

Find out more and enrol now at
www.theirm.org/digitalrisk



Contents

About the Institute of Risk Management (IRM)	4
About the Charities Special Interest Group (SIG)	4
About this guide	5
Our authors and editors	5
Purpose	5
Introduction	6
Cyber risk and the charitable sector	6
Major challenges	7
Stakeholder engagement	7
Investment and donor perceptions	8
Managing major change to infrastructure	8
Inadequate digital skills	9
Data protection outside the EU	9
Volunteers	10
Sharing sensitive data with third parties	10
Can insurance help mitigate the cost of these risks?	11
Want to learn more?	11

About the Institute of Risk Management (IRM)

The IRM is the leading professional body for Enterprise Risk Management (ERM). We drive excellence in managing risk to ensure organisations are ready for the opportunities and threats of the future. We do this by providing internationally recognised qualifications and training, publishing research and guidance, and setting professional standards.

For over 30 years our qualifications have been the global choice of qualification for risk professionals and their employers. We are a not-for-profit body, with members working in all industries, in all risk disciplines and in all sectors around the world.

About the Charities Special Interest Group (SIG)

The IRM Charities SIG was established over 10 years ago to provide practical guidance for charities about managing risk and to provide opportunities for sharing knowledge, tips and best practice amongst sector professionals.

Our overall aim is to increase the sector's knowledge of risk management best practice, explore practical solutions for managing sector challenges (such as new regulation requirements), and provide a forum where risk professionals can meet to learn from one another and share up-to-date risk management practice.

To join the Charities Special Interest Group or for additional information, please take a look at our web page: www.theirm.org/charities

About this guide

While cyber may lead organisations to think of hackers, ransomware and similar threats, risks often come from within – including from employees, volunteers, suppliers and other stakeholders all of which are the lifeblood of charitable organisations. The need to protect your organisation from the financial and reputational loss that a breach can bring is more integral than ever before and while the amount of information available to charities concerning cyber risks has greatly improved, it is still important that organisations take the time to understand where these threats emanate from and what can be done about them.

The purpose of this document is to explore the strategic cyber and digital risks faced by charitable organisations and give examples of what you can do about managing them. Representatives from several charities at an IRM Charities Special Interest Group workshop on cyber risk identified the risk themes and offered advice on how to manage the risks.

The likelihood of an organisation experiencing one of these risks will vary according to the nature of the charity and its context. Examples provided within this document are for illustrative purposes, and it will be necessary to tailor any risks and responses for your charity. Any crisis resilience plans should be regularly reviewed to ensure that they remain aligned to a charity's evolving priorities and the changing internal and external environment.

Our authors and editors

This guidance is based on the input of those members of the IRM Charities Special Interest Group (SIG) that attended the October 2018 cyber risks event.

With editing undertaken by:

Alyson Pepperill CFIRM, IRM Charities SIG Chair

Jay Sullivan, Gallagher

Roberta Beaton, Nursing Midwifery Council

Anita Punwani CFIRM, Amap Services Ltd

Purpose

This document delves into at the main challenges faced by charitable organisations: stakeholder engagement, investment and donor perception, securing data outside the EU, infrastructure changes, poor digital skills and volunteers before looking at how these risks can be managed.

Introduction

Information is a core asset of any organisation and it's important to manage and secure it properly to prevent data being accessed incorrectly or maliciously. As charities become increasingly reliant on technology, the internet and social media, they risk exposing themselves to a variety of risks including cyber-crime. Risks come from failing to keep up with technology, poor digital skills, poor controls or detection mechanisms, failing to adapt your infrastructure to change and stakeholder resistance. All of these factors can lead to your charity falling behind and losing service users, volunteers or donors, as well as failing to take advantage of new technology to fulfil your mission.

The introduction of the GDPR (General Data Protection Regulation) and a greater focus on information governance means that your charitable organisation needs to be able to react quickly in the event of a data breach. Your responsibility is to have systems in place to detect and report breaches to sector regulators such as the ICO (Information Commissioners Office) and Charity Commission using the correct channels within the allocated timescales. Failure to do so can result in fines which could potentially cripple your charity and leave you unable to fulfil your core mission. There is also the risk of failing to secure your data outside of the EU and falling foul of fines or regulatory issues other than GDPR.

Stakeholder trust is critical, as donors and service users may be discouraged from contributing if they feel that you cannot keep their data secure. Information breaches can have a significant detrimental impact on stakeholder perceptions and your charity's reputation.

The information is provided for guidance purposes only and should not be regarded as a substitute for taking specialist or legal advice.

Cyber risk and the charitable sector

Cyber is a threat which charitable organisations are understandably concerned about, yet there is a lack of knowledge and drive to tackle issues with technology within organisations. Failure to fix internal issues such as gaps in technical knowledge, awareness of security and data processes, and failing to invest in and manage changes to infrastructure can create a ticking time bomb of issues. This can result in regulatory penalties, conflict with stakeholders, and the loss and alienation of your donors.

The sector has been reluctant to spend donor's money on investing in new technology for fear of the challenge that this takes away funding from frontline services. However, as stakeholder awareness increases about data handling and ethical use more people expect charities to provide online services, and this means that organisations need to act to provide the skills, knowledge and tools to meet these expectations. With increasing pressure and a greater awareness that data is a major charitable asset, organisations are finding that there are more risks created by not taking action than investing resources.

Staff, stakeholders and volunteers need to feel empowered to use current technology and confident with adopting new systems and processes. This is a key component in successful resilience from internal and external cyber threats.

Another important factor is designing, issuing and integrating policies and processes for every facet of handling data securely from volunteer access rights through to privacy. Implementing this approach from the top down will help to build a culture of resilience, which encourages positive change with regular education of staff and volunteers to ensure that awareness remains aligned with organisational needs.

Major challenges

Our Charities Special Interest Group attendees at the meeting in October 2018 identified several areas of focus for charities to consider:

1. Stakeholder engagement

The risk

Technology related issues impact both internal and external stakeholders – not just the rapid pace of development but also an innate resistance to using new products that exists with some parts of society.

The lack of digital awareness of some trustees and the pace of decisions required, teamed with a fear of failure can pose a big challenge when it comes to the successful use of new technologies. The sheer number of technologies available can be confusing, and this means that beneficiaries often cannot afford all the digital solutions required. There is also a temptation to pick one solution without trialling and checking the others, or not co-producing designs with users.

It isn't just financial backing that breeds resistance, ICT projects take time and people to implement, which may divert resources away from business as usual or generate inertia when digital transformation takes several years to deliver.

How can this be tackled

Firstly, it is important that a digital strategy forms a part of your overall organisational strategy. Your digital strategy should consider the organisation's current state and set the desired vision for the future. This will help you to do a gap analysis to identify risks, issues and opportunities between the current and future state (taking into account ICT infrastructure, systems, policies, procedures, cyber vulnerabilities, capabilities, compliance and major controls). This analysis will shape the plan to move towards your desired state and will underpin any investment decisions but clarifying the scope, benefits and expected timeframes. It will also help you to identify which issues to monitor and how far your plan needs to look into the future.

While it can be tempting to buy-in to new technology as soon as it emerges, it's important to take small steps before committing time, resources and expense. Pilot schemes and trials are important as these allow you to make small changes and gauge stakeholder's reactions. This cautious appetite to risk should resonate with your trustees, as they need to understand what you're trying to achieve so that they can empower you and support agile decision-making. Options appraisal and benchmarking can provide useful analysis to support decision making.

Organisations should consult with their stakeholders to understand where they are in terms of technology and its potential impact. This can be a time-consuming process and may alienate people as different people adapt at different rates, so while some could feel patronised, others could feel left behind. As such, it's important to gauge reactions across your stakeholder group to ensure technology changes are proportionate, whilst keeping in mind that any solutions need to be sufficiently future proofed so that resources are not wasted in the medium term. You should also consider societal expectations when developing solutions. For example, would stakeholders expect to be able to access online services from you?

For example, the older people of today who may struggle with technology should not be the primary influence on your strategy and as the older people of tomorrow are likely to expect digital services. In this circumstance, you may need to consider traditional methods alongside developing digital ones so that stakeholders retain a choice, such as providing the elderly with technical support. Young people increasingly expect to sign in with social media accounts and don't have emails.

Please see our Stakeholder Mapping guide for more details:

<https://www.theirm.org/media/3816508/Stakeholder-mapping.pdf>

2. Investment and donor perceptions

The risk

Technology is expensive and often donors want to see their funding on ‘the front line’ instead of deploying it on ‘back room’ resources and systems.

Failure to invest can result in a loss of competitive advantage (e.g. utilising contactless fundraising boxes), a skills gap in your workforce, employees falling behind in knowledge, not retaining talented employees, or finding it difficult to attract new talent. This may mean your organisation will need to plug the gap with expensive contractors who have specialist knowledge or develop unplanned and unbudgeted rapid solutions to retain or regain competitive advantage.

How can this be tackled

Your digital strategy should be the cornerstone of any investment decisions, and should explain the both the results of taking action and the impact of not taking action such as being left behind in the sector or becoming irrelevant or less important to your clients.

Planning, undertaking a risk assessment, and prioritising how any investments are spent is vital and returns on any investment needs to be linked to your organisation’s position in the market. For example, if a competitor takes the lead could they begin to draw in donors and clients that were previously ‘yours’?

Strong communications and a phased approach are vital for building a digital culture with the skills to implement a successful digital strategy.

Provide your board of trustees with knowledge about the risks of cyber-crime and information management. And discuss with them how investment in technology and digital infrastructure can provide both opportunities to deliver your objectives as well reducing risk and improving efficiency.

3. Managing major change to infrastructure

The risk

As your organisation develops, you may need to change to bring in new opportunities and to encourage progression. Yet people are hardwired to resist change and often feel anxious about it.

Stakeholders will have requirements and expectations you need to meet. Any change in infrastructure needs the right people to make it successful and any integration requirements need assessing before they’re incorporated to ensure changes work.

How can this be tackled

Planning is crucial – you need to articulate a digital strategy and then undertake your gap analysis. You may supplement this with detailed plans about the specific change you are making and ensure that you set up appropriate governance to ensure your plans are robust. Where required you need to be aware of any regulatory issues and invest and deploy appropriate project management.

Ensure that you assess the impact on affected areas and create plans to limit business interruption. You should consider testing prior to launch either using a safe testing environment or running systems in parallel until teething problems have been resolved. Strong communications and engagement with key stakeholders will be essential and you should create a stakeholder engagement plan.

4. Inadequate digital skills

The risk

Inadequate digital skills can lead to your organisation being left behind, with the consequence of disengagement between donors, beneficiaries and your brand. Catching up can be time consuming and prohibitively expensive, and the longer its left the more likely it is your charity will stagnate and lose out.

Impact could include issues with attracting and retaining talented employees, slow progress when delivering digital transformation, using an expensive temporary workforce, and negative perceptions of your brand as 'old fashioned' or your services 'difficult to use'.

How can this be tackled

For an interim solution, perhaps you can find and encourage those with the required skills to work on pro bono terms. Look for untapped resources, for example, students who are willing to act as ethical hackers and try to hack the systems to test cyber security.

Ensure staff and volunteers are engaged and aware of the need to keep up third-party innovation. Where possible, introduce an e-learning regime to enhance skills and awareness and offer opportunities for skills development and incentives to gain experience.

Encourage the board to invest both in the infrastructure as well as developing home grown skills to reduce reliance on third party expertise.

5. Data protection outside the EU

The risk

While the focus for organisations in the EU is on GDPR, other countries and regions have their own laws such as the California Consumer Privacy Act, which became law in June 2018.

How can this be tackled

It is important to educate users, employees and volunteers about data law and culture wherever your charity operates and not just focus on GDPR if you do operate beyond the EU. While you should aim to practice a high level of data control anyway, including encryption, the range of laws and regulatory requirements make compliance especially important.

Understand where in the world your organisation operates and which laws are relevant to your service delivery. Aim to practice ethical information management and assess the risks related to hosting your information on networks outside the EU.

6. Volunteers

The risk

Even the best meaning of volunteers can find themselves victims of social engineering, and an error made by a volunteer could result in catastrophic financial and reputational damage for your organisation.

How can this be tackled

It is important that your organisation understands where and when it is appropriate to give volunteers access to potentially sensitive data and when to restrict access, by keeping them off shared drives for example. There needs to be a Volunteer Data Policy, owned by senior management and endorsed by the Board, the policy should set out the processes and procedures and how to maintain the policy, so the volunteers understand what the charity expects of them.

It may also make sense to segregate volunteering activities away from the central/core systems to keep the important data safe. You may lose some volunteers if they do not feel valued or trusted by this action, so it is vital to explain why you are taking this action and the benefits to the volunteers.

Limiting access is only one strand of a good security approach; you should also educate staff and volunteers on what they can and cannot do. You should consider incorporating technology with built-in access limits and investigate technology monitoring systems which could enforce this. For example, utilising technology to wipe company email accounts and clear cache data remotely if there is a risk of a breach.

7. Sharing sensitive data with third parties

The risk

All charitable organisations have sensitive data, and it's important that the only people who see this are those on a need-to-know basis. Failure to do so can result in negative publicity and a loss of trust from your donors, clients, and the public.

How can this be tackled

Once again, it is important to have policies in place including policies that cover governance, data, HR and information security. There needs to be a top down messaging campaign to encourage a culture of security; this process should ensure legal messages are sent out from a central source and that local offices know what they can and can't do. This can be reinforced with technology, for example IT can manage certain software and apps. It is not enough to rely on IT to enforce this. You need to take time and train your people in how to classify documents, understand what is confidential and who owns the document.

Security controls and detection software can support this. More important is creating a culture of information management where data is considered an important asset and people are encouraged to report and learn from when things go wrong rather than being defensive or trying to cover up mistakes.

Can insurance help mitigate the cost of these risks?

Of course, you cannot prepare yourself for every eventuality, which is where a cyber insurance policy comes highly recommended. Cyber insurance offers first and third party loss covering a range of scenarios including data breach, cyber extortion, the cost of breach notifications, hacking and many more whether due to accidental acts of volunteers or more malicious and deliberate acts of disgruntled ex-employees or other third parties. In short, it can help you respond when the unexpected happens.

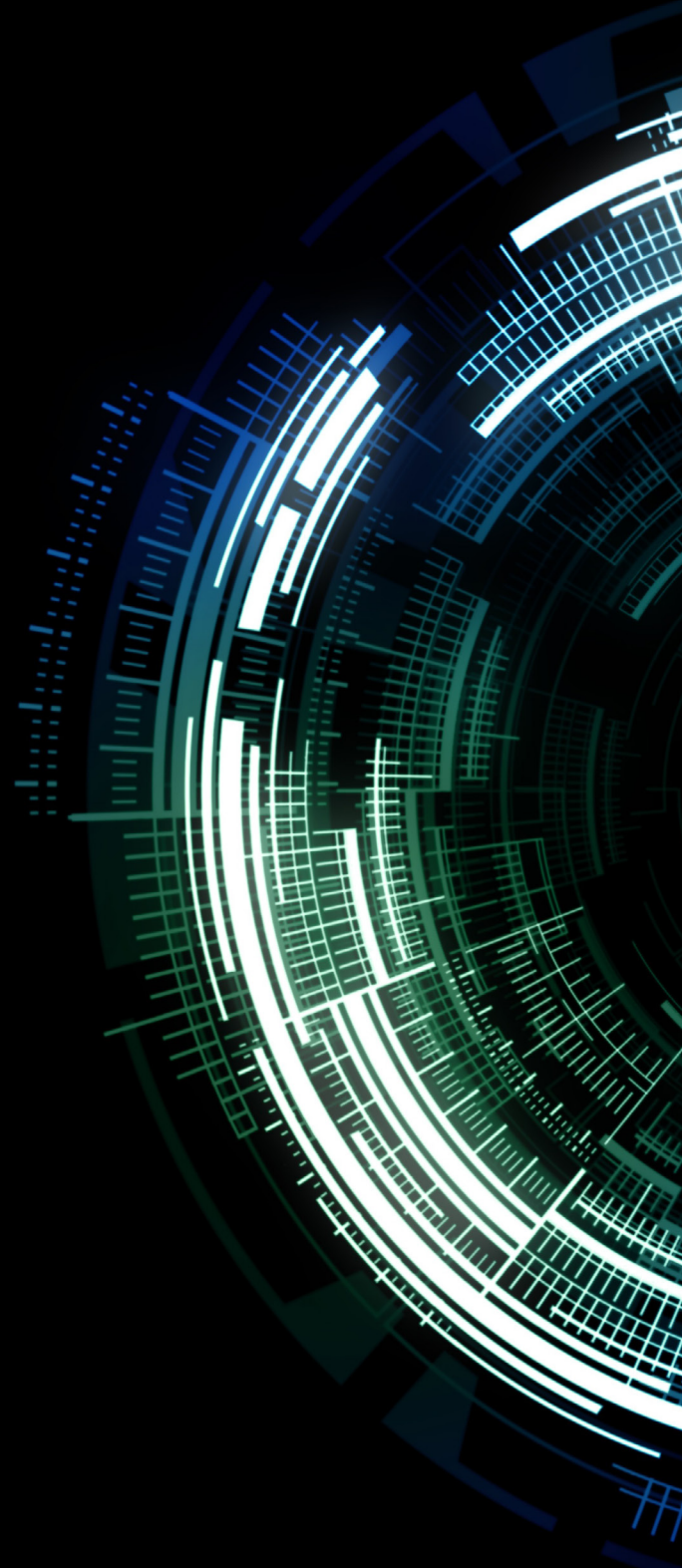
Insurance not only provides funds to respond to an event but as Alyson Pepperill CFIRM of Gallagher explains, will also provide access to specialists who can help you recover as quickly as possible: “An insurance policy provides access to a panel of quality specialist IT and other contractors who are dealing with events for insurers on a daily basis. Deployment of people with experience and expertise who can tackle the incident quickly will help to limit the financial and reputational damage arising from the event. Once the excess has been paid it is the insurance company who will cover the costs of the experts keeping your funds for your core mission.”

Want to learn more?

The IRM has a Cyber and Information Management SIG that you may like to join. The IRM and the SIG have published several useful guides. We recommend:

- IRM cyber resilience guidance: <https://www.theirm.org/knowledge-and-resources/thought-leadership/cyber-risk/>
- <https://www.theirm.org/media/3814330/IRM-Cyber-Risk-Resources-for-Practitioners.pdf>

The National Cyber Security Centre is also a good source of information: <https://www.ncsc.gov.uk/>



Institute of Risk Management
2nd Floor, Sackville House
143–149 Fenchurch Street
London
EC3M 6BN

www.theirm.org



Developing risk professionals