Cyber risk management

UK CHARITY SECTOR

ecclesiastical

Cyber risk management for charities

Introduction

Charities face a myriad of challenging hazards and threats and they now have to prepare for human-caused cyber threats. These incidents can be accidental or deliberate and disrupt critical operations; expose sensitive personally identifiable information (PII) of beneficiaries, donor, trustees, patrons, partners, paid staff and volunteers.

This report is not written from a technical perspective. Instead, it looks at the management steps that are required across the whole charity in order to be cyber secure. It primarily focuses on the challenge of protecting against targeted, unauthorised attempts to access digital information, including research.

Cyber threats can impact either the human (beneficiaries, donors, trustees, patrons, partners, paid staff and volunteers) or the physical or virtual (e.g. information technology [IT] networks and systems) elements. While there may be some overlap in addressing human versus physical/virtual threats, preparing for each type can require input from different individuals with experience or expertise on that topic and unique actions before, during, and after an incident. Charities may therefore choose to plan for these threats separately, but still under a broader umbrella of cyber threats.

The cyber threats facing charities are varied. There are a variety of general threats to a charity and its infrastructure, such as through distributed denial of service attacks (DDoS) that may directly or indirectly target a charity's network. General criminal and fraudulent threats target users in order to obtain personal data for identity fraud or financial theft. There are also increasingly targeted attempts to obtain potentially sensitive data which may include personal data of beneficiaries, donors, staff and volunteers or certain types of information, such as research, for commercial or political means.

Treatment of the risk

The starting point of risk management is an acceptance that risk can't simply be abolished. Risk must be recognised and then managed in some way or other (classically to either **avoid**, **reduce**, **transfer** or **retain**). This can be easier said than done, particularly when confronted with a demand to 'abolish risk', as if that were an easy and simple option.

There are four ways you can treat a risk:

Generally, you need to do everything 'reasonably practicable' to protect the charity from harm.

This means balancing the level of risk against the measures needed to control the real risk in terms of money, time or trouble. However, you do not need to take action if it would be grossly disproportionate to the level of risk.

Look at what you're already doing and the control measures you already have in place. Ask yourself if you can get rid of the hazard altogether?

If not, how can you control the risks so that damage or loss is unlikely?

1. Avoid the risk

The easiest way for a charity to manage its identified risk is to avoid it altogether. In its most common form, avoidance takes place when a charity ceases any activities known or perceived to carry a risk of any kind. However, in some instances, avoiding risk in its entirety is not possible without impeding the smooth running of the charity.

2. Reducing the risk

The following advice has been produced by the NCSC (National Cyber Security Centre, a part of GCHQ). Following this advice will significantly increase your protection from the most common types of cyber attack.

National Cyber Security Centre
a part of GCHQ

The topics covered are easy to understand and cost little to implement. This advice can't guarantee protection from all types of cyber attack, but it does show how easy it can be to protect your charity's data, assets, and reputation.

Backing up your data

All charities, regardless of size, should take regular backups of their important data, and make sure that these backups are recent and can be restored. By doing this, you are ensuring your charity can still function following the impact of a cyber attack or flood, fire, physical damage or theft.

Furthermore, if you have backups of your data that you can quickly recover, you can't be the victim of extortion by Ransomware attacks.

1. Identify what data you need to back up

Your first step is to identify your essential data. That is, the information that your charity couldn't function without. Normally this will comprise donor and staff/volunteer records, images, emails, contacts, and calendars, most of which are kept in just a few common folders on your network, computers, phones or tablets.

2. Keep your backup separate from your computer

Whether it's on a separate drive or a separate computer, access to data backups should be restricted so that they:

- are not accessible by staff
- are not permanently connected (either physically or over a local network) to the device holding the original copy.

Ransomware (and other malware) can often move to attached storage automatically, which means any such backup could also be infected, leaving you with no backup to recover from. For more resilience, you should consider storing your backups in a different location, so fire or theft won't result in you losing both copies. Cloud storage solutions (see below) can be a cost-effective and efficient way of achieving this.

3. Consider the cloud

Cloud computing (externally hosted servers) is increasing in popularity and according to the Advanced Trends Report 2017, 65% of charities use Cloud-based technology. Cloud computing can offer a charity a convenient low cost way to connect multiple offices, improve communication, regularly back up their systems and deliver services more efficiently.

Using cloud storage (where a service provider stores your data on their infrastructure) means your data is physically separate from your location. You'll also benefit from a high level of availability. Service providers can supply your charity with data storage and web services without you needing to invest in expensive hardware up front. Most providers offer a limited amount of storage space for free, and larger storage capacity for minimal costs.

However, it should be remembered that a cloud server is still ‘someone else’s computer’ and not all service providers are the same. But the market is reasonably mature and most providers have good security practices built-in. However, before contacting service providers, we encourage you to read the NCSC's Cloud Security Guidance.

4. Make backing up part of your everyday business

We know that backing up is not a very interesting thing to do (and there will always be more important tasks that you feel should take priority), but the majority of network or cloud storage solutions now allow you to make backups automatically. For instance, when new files of a certain type are saved to specified folders. Using automated backups not only saves time, but also ensures that you have the latest version of your files should you need them.

Many off-the-shelf backup solutions are easy to set up, and are affordable considering the business-critical protection they offer. When choosing a solution, you'll also have to consider how much data you need to back up, and how quickly you need to be able to access the data following any incident.

Protecting your charity from malware

Your systems may be damaged, have access denied or even destroyed by the use of malicious software, known as Malware, that can spread throughout a network. Such incidents can incur expense in repairing damage to your charities computer systems including websites.

1. Install (and turn on) anti-malware software

Anti-Malware (also referred to as Anti-virus) software - should be used on all computers and laptops.

However, signature based anti-malware software could also be considered. Many of the current applications rely on recognising the Malware from an extensive database and as a result it can only detect and stop what it knows. A number of Ransomware variants have been seen that have able to pass through without detection. Behaviour based detection is an additional feature that some anti-malware providers offer and can stop Ransomware when it attempts to encrypt your files.

2. Prevent trustees, volunteers or staff from downloading potentially harmful apps

You should only download apps for mobile phones and tablets from manufacturer-approved stores (like Google Play or Apple App Store). These apps are checked to provide a certain level of protection from malware that might cause harm. You should prevent staff from downloading third party apps from unknown vendors/sources, as these will not have been checked.

Staff accounts should only have enough access required to perform their role, with extra permissions (i.e. for administrators) only given to those who need it. When administrative accounts are created, they should only be used for that specific task, with standard user accounts used for general work.

3. Keep all your IT equipment up to date (patching)

For all your IT equipment (so tablets, smartphones, laptops and PCs), make sure that the software and operating system is always kept up to date with the latest versions from software developers, hardware suppliers and vendors. Applying these updates (a process known as patching) is one of the most important things you can do to improve security. Operating systems, programmes, phones and apps should all be set to 'automatically update' wherever this is an option.

At some point, these updates will no longer be available (as the product reaches the end of its supported life), at which point you should consider replacing it with a modern alternative.

4. Control how USB or cards drives can be used

We all know how tempting it is to use USB drives or memory cards to transfer files between volunteers, staff and the charity. However, it only takes a single cavalier user to inadvertently plug in an infected stick (such as a USB drive containing malware) to devastate the whole charity.

When USB drives or memory cards are openly shared, it becomes hard to track what they contain, where they've been, and who has used them. You can reduce the likelihood of infection by:

- blocking access to physical ports for most users
- using anti-malware tools
- only allowing approved USB drives or memory to be used within the charity - and nowhere else.

Make these directives part of your charity's policies and procedures, to prevent it being exposed to unnecessary risks. You can also ask trustees, volunteers or staff to transfer files using alternate means (such as by email or cloud storage), rather than via USB.

5. Switch on your firewall

Firewalls create a 'buffer zone' between your charity's network and external networks (such as the Internet). Most popular operating systems now include a firewall, so it may simply be a case of switching this on.

Keeping your smartphones (and tablets) safe

With limited resources charities may not be able to offer modern equipment to their staff and volunteers. BYOD or Bring Your Own Device is a convenient way to give staff access to emails and the network. 61% of staff at charities regularly use personal devices for charity work*. Unless these devices are correctly configured they can leave a charity open and vulnerable.

1. Switch on password protection

A suitably complex PIN or password (opposed to a simple one that can be easily guessed or gleaned from your social media profiles) will prevent the average criminal from accessing your phone. Many devices now include fingerprint recognition to lock your device, without the need for a password. However, these features are not always enabled 'out of the box', so you should always check they have been switched on.

2. Make sure lost or stolen devices can be tracked, locked or wiped

Staff are more likely to have their tablets or phones stolen (or lose them) when they are away from the charity or home. Fortunately, the majority of devices include free web-based tools that are invaluable should you lose your device. You can use them to:

- track the location of a device
- remotely lock access to the device (to prevent anyone else using it)
- remotely erase the data stored on the device
- retrieve a backup of data stored on the device

Setting up these tools on all your charity's devices may seem daunting at first, but by using mobile device management software, you can set up your devices to a standard configuration with a single click.

3. Keep your device up-to-date

No matter what phones or tablets your organisation is using, it is important that they are kept up to date at all times. All manufacturers (for example Windows, Android, iOS) release regular updates that contain critical security updates to keep the device protected.

This process is quick, easy, and free; devices should be set to automatically update, where possible. Make sure your staff know how important these updates are, and explain how to do it, if necessary. At some point, these updates will no longer be available (as the device reaches the end of its supported life), at which point you should consider replacing it with a modern alternative.

4. Keep your apps up-to-date

Just like the operating systems on your organisation's devices, all the applications that you have installed should also be updated regularly with patches from the software developers. These updates will not only add new features, but they will also patch any security holes that have been discovered. Make sure staff know when updates are ready, how to install them, and that it's important to do so straight away.

*Source: Department for Digital, Culture, Media & Sport - Cyber Security Breaches Survey 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdf

5. Don't connect to unknown Wi-Fi hotspots

When you use public Wi-Fi hotspots (for example in hotels or coffee shops), there is no way to easily find out who controls the hotspot, or to prove that it belongs to who you think it does. If you connect to these hotspots, somebody else could access:

- what you're working on whilst connected
- your private login details that many apps and web services maintain whilst you're logged on.

The simplest precaution is not to connect to the Internet using unknown hotspots, and instead use your mobile 3G or 4G mobile network, which will have built-in security. This means you can also use 'tethering' (where your other devices such as laptops share your 3G/4G connection), or a wireless 'dongle' provided by your mobile network.

You can also use Virtual Private Networks (VPNs), a technique that encrypts your data before it is sent across the Internet. If you're using third party VPNs, you'll need the technical ability to configure it yourself, and should only use VPNs provided by reputable service providers.

Using passwords to protect your data

1. Make sure you switch on password protection

Set a screen lock password, PIN, or other authentication method (such as fingerprint or face unlock). If you're mostly using fingerprint or face unlock, you'll be entering a password less often, so consider setting up a long password that's difficult to guess.

Having said this, password protection is not just for smartphones and tablets. Make sure that your office equipment (so laptops and PCs) all use an encryption product (such as BitLocker for Windows) with a PIN, or FileVault (on macOS) in order to start up. Most modern devices have encryption built in, but encryption may still need to be turned on and configured, so check you have set it up.

2. Use two-factor authentication for 'important' accounts

If you're given the option to use two-factor authentication (also known as 2FA) for any of your accounts, you should do; it adds a large amount of security for not much extra effort. 2FA requires two different methods to 'prove' your identity before you can use a service, generally a password plus one other method. This could be a code that's sent to your smartphone (or a code that's generated from a bank's card reader) that you must enter in addition to your password.

3. Avoid using predictable passwords

Make sure staff are given actionable information on setting passwords that is easy for them to understand.

Passwords should be easy to remember, but hard for somebody else to guess. A good rule is make sure that somebody who knows you well, couldn't guess your password in 20 attempts'. Staff should also avoid using the most common passwords, which criminals can easily guess. The NCSC has some useful advice on how to choose a non-predictable password.

4. Help your staff cope with 'password overload'

There's a number of things you can do that will improve security. Most importantly, your staff will have dozens of non-work related passwords to remember as well, so only enforce password access to a service if you really need to.

Where you do use passwords to access a service, do not enforce regular password changes. Passwords really only need to be changed when you suspect a compromise of the login credentials. You should also provide secure storage so staff can write down passwords for important accounts (such as email and banking), and keep them safe (but not with the device itself). Staff will forget passwords, so make sure they can reset their own passwords easily.

Consider using password managers, which are tools that can create and store passwords for you that you access via a 'master' password. Since the master password is protecting all of your other passwords, make sure it's a strong one, for example by using three random words.

5. Change all default passwords

One of the most common mistakes is not changing the manufacturers' default passwords that smartphones, laptops, and other types of equipment are issued with. Change all default passwords before devices are distributed to staff.

Avoiding phishing attacks

In a typical phishing attack, scammers send fake emails to thousands of people, asking for sensitive information (such as bank details), or containing links to bad websites. They might try to trick you into sending money, steal your details to sell on or have political or ideological motives for wanting your charities data.

Phishing emails are getting harder to spot, and some will still get past even the most observant users.

1. Configure accounts to reduce the impact of successful attacks

You should configure your staff and volunteer accounts in advance using the principle of 'least privilege'. This means giving staff the lowest level of user rights required to perform their jobs, so if they are the victim of a phishing attack, the potential damage is reduced. To further reduce the damage that can be done by malware or loss of login details, ensure that your staff don't browse the web or check emails from an account with Administrator privileges.

An Administrator account is a user account that allows you to make changes that will affect other users. Administrators can change security settings, install software and hardware, and access all files on the computer. So an attacker having unauthorised access to an Administrator account can be far more damaging than accessing a standard user account.

2. Think about how you operate

Consider ways that someone might target your organisation, and make sure your trustees, staff and volunteers all understand normal ways of working (especially regarding interaction with other organisations), so that they're better equipped to spot requests that are out of the ordinary.

Think about your usual working practices and how you can help make these tricks less likely to succeed. For example:

- Do trustees, staff and volunteers know what to do with unusual requests, and where to get help?
- Ask yourself whether someone impersonating an important individual (a trustee, beneficiary or manager) via email should be challenged (or have their identity verified another way) before action is taken.
- Do you understand the day to day charity relationships your charity has? Scammers will often send phishing emails from large organisations (such as banks) in the hope that some of the email recipients will have a connection to that company. If you get an email from an organisation you don't do business with, treat it with suspicion.
- Think about how you can encourage and support your staff to question suspicious or just unusual requests – even if they appear to be from important individuals. Having the confidence to ask 'is this genuine?' can be the difference between staying safe, or a costly mishap.

You might also consider looking at how your outgoing communications appear to trustees, staff and volunteers. Will your emails get mistaken for phishing emails, or leave people vulnerable to an attack that's been designed to look like an email from you? Consider telling your suppliers or customers of what they should look out for (such as 'our bank details will not change at any point').

3. Check for the obvious signs of phishing

Expecting your staff to identify and delete all phishing emails is an impossible request and would have a massive detrimental effect on charity productivity. However, many phishing emails still fit the mould of a traditional attack, so look for the following warning signs:

- Many phishing scams originate overseas and often the spelling, grammar and punctuation are poor. Others will try and create official-looking emails by including logos and graphics. Is the design (and quality) what would you'd expect from a large organisation?
- Is it addressed to you by name, or does it refer to 'valued customer', or 'friend', or 'colleague'? This can be a sign that the sender does not actually know you, and that it is part of a phishing scam
- Does the email contain a veiled threat that asks you to act urgently? Be suspicious of words like 'send these details within 24 hours' or 'you have been a victim of crime, click here immediately'
- Look out for emails that appear to come from a senior person within the charity, requesting a payment is made to a particular bank account. Look at the sender's name. Does it sound legitimate, or is it trying to mimic someone you know?
- If it sounds too good to be true, it probably is. It's most unlikely that someone will want to give you money, or give you access to some secret part of the Internet.

Email filtering services attempt to send phishing emails to spam/junk folders. However, the rules determining this filtering need to be fine-tuned for your charities needs.

If these rules are too open and suspicious emails are not sent to spam/junk folders, then users will have to manage a large number of emails, adding to their workload and leaving open the possibility of a click. However, if your rules are too strict, some legitimate emails could get lost. You may have to change the rules over time to ensure the best compromise.

4. Report all attacks

Make sure that your trustees, staff and volunteers are encouraged to ask for help if they think that they might have been a victim of phishing, especially if they've not raised it before. It's important to take steps to scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred.

Do not punish staff if they get caught out. It discourages people from reporting in future, and can make them so fearful that they spend excessive time and energy scrutinising every single email they receive. Both these things cause more harm to your charity in the long run. You should also report it as a serious incident to the Charity Commission via RSI@charitycommission.gsi.gov.uk, or the Office of the Scottish Charity Regulator (OSCR) in Scotland.

Reporting demonstrates that you have taken responsible action to identify problems within your charity. It also helps the Commission to gauge threats that may affect the wider sector, and to take steps to address these with targeted advice and guidance.

5. Check your digital footprint

Attackers use publicly available information about your charity and staff to make their spear phishing messages more convincing. This is often gleaned from your charity's website and social media accounts (information known as a 'digital footprint').

- Understand the impact of information shared on your charity's website and social media pages. What do visitors to your website need to know, and what detail is unnecessary (but could be useful for attackers)?
- Be aware of what your partners, contractors and suppliers give away about your charity online
- Help your staff understand how sharing their personal information can affect them and your charity. This is not about expecting people to remove all traces of themselves from the Internet. Instead support them as they manage their digital footprint, shaping their profile so that it works for them and the organisation
- The Centre for the Protection of National Infrastructure's (CPNI) Digital Footprint Campaign contains a range of useful materials (including posters and booklets) to help organisations work with employees to minimise online security risks

3. Transfer the risk

Risk transfer is a risk management strategy that involves the contractual shifting of a risk from one party to another. One example is the purchase of an insurance policy, by which a specified risk of loss is passed from you to the insurer.

Cyber insurance acts as a safety net. As we mentioned, it's impossible to completely eliminate cyber risks even with sophisticated cyber security controls in place.

What does cyber insurance cover?

Ecclesiastical's cyber insurance for charities includes the following cover:

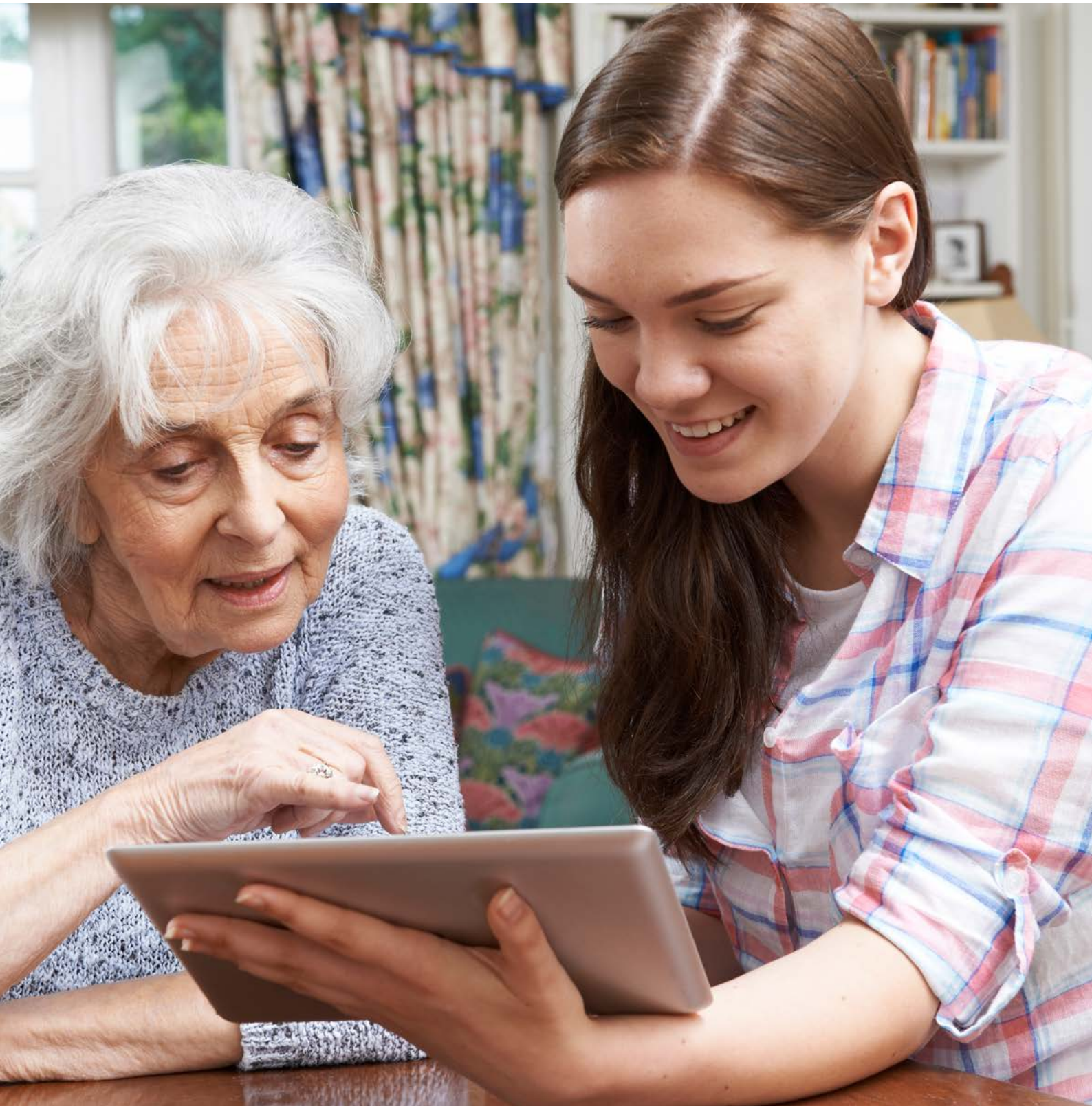
- Damage to computer hardware
- Restoration of lost or corrupted data
- Cover that helps organisations with the impact of cyber crime such fund transfer fraud, computer enabled fraud or cyber extortion plus:
  - Network charges following telephone system hacking
  - Specialist support following a cyber extortion threat
- Costs of dealing with cyber liability claims plus:
  - Liability arising from libel/slander or loss of intellectual property rights
  - Onward transmission of malware
- Costs of dealing with data breaches (excluding legal nes)
  - Legal and forensic IT review
  - Notification costs to the regulator
  - Costs to provide ID assistance, credit monitoring and help lines to affected parties
  - Public relations and crisis management expenses
- Cover for charity's fee income lost as the result of a cyber event.

It also includes access to expert advice and support when an incident occurs to help mitigate the nancial impact or reputational damage.

4. Retain the risk

Planned acceptance of risks by excesses or deliberate non-insurance, where some, but not all, risk is consciously retained rather than transferred.

This is a good strategy to use for very low risks – risks that won't have much of an impact on your charity if they happen and could be easily dealt with if or when they arise.



Useful links

www.actionfraud.police.uk
(The National Fraud & Cyber Crime Reporting Centre. Cyber crimes committed or attempted against you can be reported here. Also contains useful information on how to protect your charity against fraud, scam emails etc)

www.ncsc.gov.uk/guidance
(Website for the National Cyber Security Centre, useful information on how to protect your charity against common cyber threats)

www.gov.uk/data-protection/the-data-protection-act
(Overview of the Data Protection Act 1998)

www.ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/
(Information about the General Data Protection Regulation (GDPR) affecting UK law from May 2018)

www.iso.org/isoiec-27001-information-security.html
(Website for the International Organisation for Standardization who developed ISO/IEC 27001:2013 referenced above)

www.riscauthority.co.uk/free-document-library/RISCAuthority-Library_detail.s28-cyber-crime-overview-and-sources-of-support.html
(Website for Riscauthority – free download document regarding cyber threats)

www.ncsc.gov.uk/cisp
(CiSP is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, con dential and dynamic environment, increasing situational awareness and reducing the impact on UK business).

If you need to improve your cyber security further, then you can also seek certi cation under the Government's Cyber Essentials scheme, which has the bene t of demonstrating to both existing and prospective clients that you take the protection of their data seriously.

See **www.cyberessentials.ncsc.gov.uk** for more details.

If you are a larger charity, or face a much greater risk from cyber crime, then the NCSC's 10 Steps to Cyber Security is a good source of information and can further enhance your approach to cyber security (**www.ncsc.gov.uk/guidance/10-steps-cyber-security**).

Compliance or alignment with a recognised standard, such as ISO/IEC 27001:2013 Information Security Management, can help you implement some of the above steps.

Insurance that is anything but ordinary

The difference is doing what's expected, and then adding extra.

Our charitable ownership gives us a greater insight into some of the challenges facing the sector. This level of understanding means we are able to support our charity customers in many ways - regulation, tax, compliance and risk management to name just a few.

To find out more visit **www.ecclesiastical.com/charity**

Ecclesiastical Insurance Office plc (EIO) Reg. No. 24869. Registered in England at Benefact House, 2000 Pioneer Avenue, Gloucester Business Park, Brockworth, Gloucester, GL3 4AW, United Kingdom. EIO is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Firm Reference Number 113848

PDXXXX 1 02/20