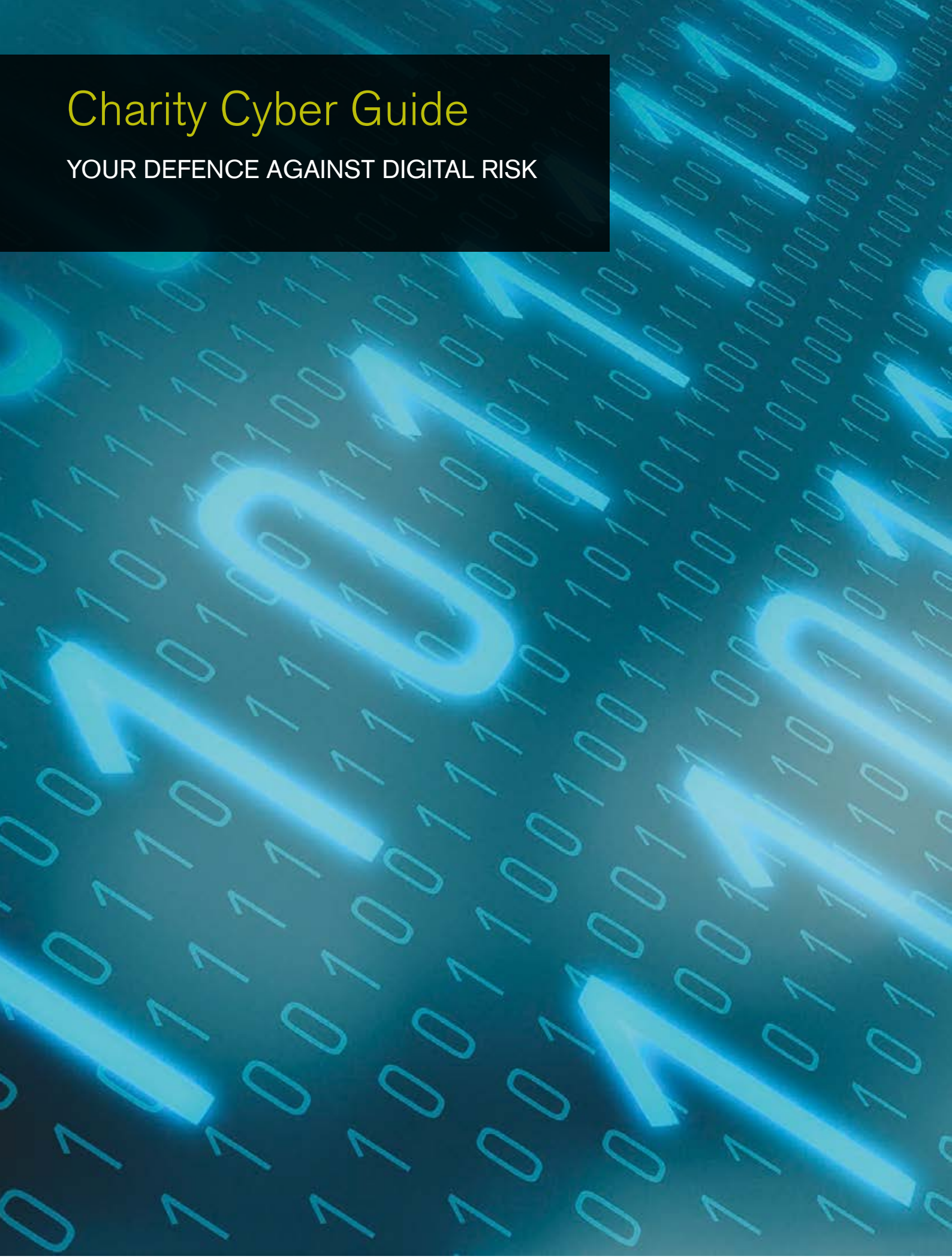
Charity Cyber Guide

YOUR DEFENCE AGAINST DIGITAL RISK



When it feels irreplaceable, trust Ecclesiastical

Digital technology has enabled charities to do more

It has created opportunities for innovative new fundraising ideas, helped save time and resource and allowed us to store information more efficiently than ever before.

On the other hand, the relentless evolution of cyber crime has highlighted the many vulnerabilities which exist for organisations and individuals alike.

Charities are no exception. The Information Commissioner's Office (ICO) statistics show that the number of charities experiencing a data breach incident has increased by two thirds on an annual basis (April 2016-17 compared to April 2015-16).[1]

In 2016, the National Crime Agency reported that cyber-related crimes had exceeded the level of physical crimes committed and it accounted for 36% of all cyber crime.[2]

This guide covers some of the risks and opportunities presented by embracing digital solutions.

"There's no doubt that the threat of a cyber-attack has become very real for charities; and that the threat will only continue to grow as these attacks increase in number, scale and ingenuity.

Representing information security people working in charities and not-for-profits, the Charities Security Forum is committed to continuing to raise awareness of cyber risk in the third sector and to help support these organisations in building up their digital defences.

This new guide by Ecclesiastical provides accessible information about the ways in which charities could find themselves exposed to the cybersecurity threat, but also gives simple, practical advice to help third sector organisations to protect themselves, and the people they help, against cyber crime."

Brian Shorten and Martyn Croft, co-founders of the Charities Security Forum

[1] https://ico.org.uk/action-weve-taken/data-security-incident-trends/
[2] http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file

Contents

David Britton
Charity Director

Cyber risk has been one of the top concerns for our charity customers for the last few years. As such, we're delighted to share this resource to help raise awareness among charities. It takes a close look at the implications of cyber crime on not-for-profits and provides some of the solutions to help keep charities and not-for-profit groups protected.

Attacks on charities

There is a common misconception that it is generally larger organisations that are targeted by cyber crime but this is not always the case.

The National Cyber Security Centre identifies charities as having the same risk as businesses saying: "Charities are subject to the same cyber vulnerabilities as other organisations and businesses that conduct financial transactions, and rely on electronically held data or information to conduct day-to-day operations."

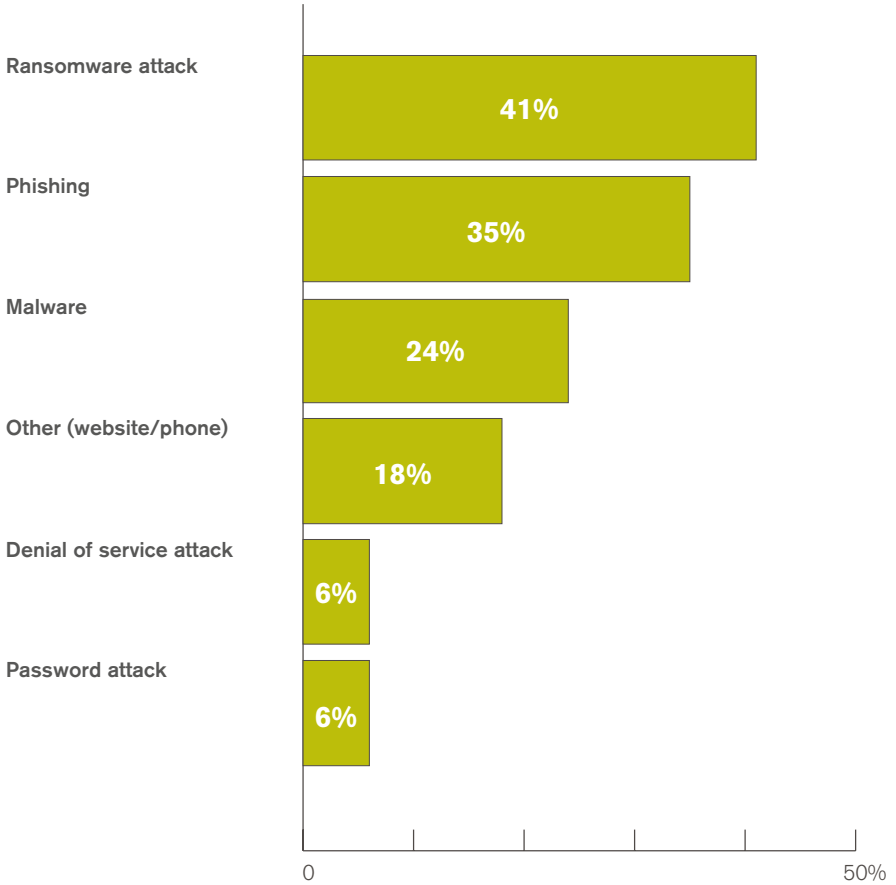
In the Government's 2017 Cyber Security Breaches Survey, 39% of Micro and Small Businesses with no governance or risk management measures in place think that they are too small or insignificant to need cyber security.

You may think that cyber criminals would have more to gain financially from attacking a larger organisation but, when you think about it, who is the easier target?

Lloyds Banking Group conducts an annual survey to assess the digital maturity of charities. In 2017, the UK Business Digital Index found that 49% of charities lack basic digital skills and more than 75% do not intend to invest money in this area.[4]

In our 2017 charity survey [3], we asked how many charities had experienced a cyber attack and which were the most common.

A total of 17% of charities said they had experienced an attack and the most frequent were:



Percentage of charities who have experienced the type of attack

[3] Ecclesiastical Annual Charity Tracking Survey 2017 by independent research agency FWD
[4] http://resources.lloydsbank.com/insight/uk-business-digital-index/

1. Ransomware

Ransomware is the most common cyber attack experienced by the charities we surveyed.

It can be very difficult to defend against a ransomware attack as the system can become infected even without user action. Ransomware simply scours the net looking for software which has a specific vulnerability.

How does ransomware work?

Ransomware attacks lock a computer or the files held on the system using strong encryption methods. The organisation is then held to ransom for the return of access to their system.

The hacker usually imposes a time limit and if you don't pay in time, your data may be gone for good.

Ransomware examples

The now famous Wannacry attack, which hit organisations including the NHS, was not targeted at any specific entity. The attack sought to expose systems which had a particular vulnerability. It affected 200,000 organisations in 150 countries worldwide.[5]

Comic Relief

Comic Relief were hit by a ransomware attack in 2016. Their systems were hacked and a proportion of their data was encrypted. Luckily, Comic Relief had their data backed up and stored it elsewhere so they did not lose any data.[6]

So should you pay a ransom?

No. Ransoms are usually demanded in Bitcoins or other forms of cryptocurrency. Some businesses have started to stockpile Bitcoins in case of a ransomware attack.

But in more than half of cases, the decryption key is not received when the ransom has been paid.[7]

Keeping machines patched with the latest updates should deal with the vulnerabilities that are exploited by the malware. Try to avoid opening attachments from unknown senders too. Even if it looks legitimate you should double-check the sender's address to be sure.

Tackling ransomware

As cyber crime is ever-evolving, and quickly, new vulnerabilities are exposed in various different software programmes every day.

Equally, there are people seeking out these vulnerabilities and fixing them. Software updates introduce fixes to vulnerabilities in your system and are called patches.

Automatic updates are a great way to ensure software is updated on a regular basis and can usually be organised quickly and easily by changing your computer settings.

Like Comic Relief, charities should back up their data to avoid losing it altogether. The first step is to identify what needs to be backed up and then ensure the device isn't permanently connected to the system. Cloud storage is also an option and you will be able to access it remotely. The National Cyber Security Centre (NCSC) have some detailed advice on backing up charity data in their cyber security guide for small charities.

[5] https://www.wired.com/2017/05/wannacry-ransomware-hackers-made-real-amateur-mistakes/
[6] https://www.theregister.co.uk/2016/09/16/comic_relief_ransomware/
[7] https://www.loricainsurance.com/legacy/documents/Newsletter-Cyber-Jan.Feb17.pdf

2. Phishing

Action Fraud receives around 8,000 reports of phishing attacks on charities per month.

The Charity Commission has recently issued an alert following increasing reports of phishing scams.

What is phishing?

Phishing describes cyber attacks which infiltrate systems via email or telephone. Cyber criminals use false pretences, such as imitation of a known brand, primarily to trick individuals into divulging personal information like bank details.

This is a particularly pertinent issue for charities where hackers mimic the charity brand and encourage donors to click a link which takes them to a bogus website to donate.

Phishing comes in other forms including:
Vishing - phishing, but via the telephone
Spear phishing - phishing where the attacker already has some information about the charity and they can use this information to initiate contact - i.e. sending an email from the bank you are with
Whaling - specifically targeting a board member or other high-earning individual within the charity.

NCSC share an example of a charity CEO who was hacked in a whaling attack. A fraudulent message was sent to the charity's finance manager, supposedly from the CEO and requesting a release of funds. £13,000 was unintentionally sent to the hacker.

Her Majesty's Revenue and Customs (HMRC)

HMRC is frequently mimicked by cyber criminals.

To try and help people to recognise what cyber crime looks like, HMRC have a webpage dedicated to highlighting the types of scam cyber criminals could attempt.

Below are examples of bogus email addresses used by scammers:

- service.refund@hmrc.gov
- taxrefund@hmrc.gov.uk
- refund-help@hmrc.gov.uk[8]

What does this mean for charities?

Education can often be the best way to prevent a phishing scam from succeeding.

All employees, including temporary staff and volunteers, should learn how to recognise suspicious messages for obvious signs of phishing and take appropriate action.

Having a high turnover of temporary employees and volunteers can be a challenge, especially when it comes to taking the time to train them.

Training and creation of an internet policy (which we will discuss later in more detail) can help educate employees and prevent phishing attacks from succeeding.

8 https://www.gov.uk/government/publications/phishing-and-bogus-emails-hm-revenue-and-customs-examples/phishing-emails-and-bogus-contact-hm-revenue-and-customs-examples

3. Malware

What is malware?

Malware stands for malicious software and is designed with the intent to steal or destroy data or damage a computer system.

It can be concealed in an email attachment, link, pop up, on a webpage or on storage devices, such as USB sticks. When these are opened, malware can then spread.

One of the most common types of malware attack is known as a worm. A worm will spread through a network and cause problems without any user interaction.

Malware warning signs

It can be hard to tell if malware is present on your system.
What are the warning signs?

- Loss of access to data
- Slow running systems
- Applications won't open
- Unusual error messages
- Notifications from anti-virus software

Microsoft give a helpful overview of how to detect malware symptoms.

How to prevent malware attacks

You should always be careful when downloading files, making sure you have confidence in the provider before you do so.

Use anti-virus software on all computers and laptops and only install approved software from known sources.

More often than not, malware attacks are made possible through phishing. As we mentioned earlier on, you can help staff and volunteers by teaching them how to spot suspicious emails.

Charity cyber insurance

It is a common condition in cyber insurance products that you must be protected by anti-virus software which is regularly updated.

4. DoS and DDoS

DoS stands for Denial of Service and DDoS stands for Distributed Denial of Service.

Both DoS and DDoS attacks focus on disrupting web services so they are temporarily unavailable. Cyber criminals do this by flooding the web server with bogus requests in an attempt to overload the system, thus preventing genuine requests from getting through.

What is the difference between DoS and DDoS?

A DoS attack is typically run from just one computer, where as a DDoS attack is made up of multiple systems in a 'botnet'.

Botnets – 'zombie armies'

Any device connected to the internet that is not properly configured or protected can be hijacked with malware without the user knowing. For example, laptops used to collect leads for the charity may still operate correctly but in the background, malware could be lurking. Downloading dodgy apps can also let malware creep on to your system. It's advisable to only use reputable stores like Google Play or the Apple App Store and always read the reviews.

The malware may lie dormant until a time when a hacker decides to remotely control the device and use it in an attack. The hacker would order the devices to submit multiple requests to a website, thereby initiating a DDoS attack. The enslaved devices are referred to as 'zombies' and a collection of infected devices is known as a botnet.

Most famously, PayPal and Twitter were hit by a huge DDoS attack in 2016. Malware spread to more than 500,000 devices and involved around 100,000 Internet connected bots.[9]

[9] https://www.pcworld.com/article/3135273/security/fridays-ddos-attack-came-from-100000-infected-devices.html

Defending against DoS and DDoS attacks

1. Create an action plan in advance
2. Monitor web traffic levels and have a method to generate alerts that recognise abnormal levels
3. Turn off connected devices when not in use
4. Change any device default passwords set by the manufacturer
5. Install patches and updates frequently
6. Consider obtaining additional bandwidth from your service provider. It might not stop the attack but it might buy you crucial time.

5. Password attacks

Technology makes it amazingly easy to crack some passwords.

What is a password attack?

A password attack aims to infiltrate a system by learning a user's password.

Brute force attacks use automated software to guess passwords over and over again until they succeed.

Dictionary attacks try thousands of combinations of letters per minute until they find the right one. Passwords like '123456' or 'password' can be hacked in less than a second.

Many organisations set rules around password length and combination of characters to ensure their system users have strong passwords which ultimately could take an infinite amount of time to hack.

Unfortunately, as with most tactics used to defend against cyber attacks, there are other ways to crack passwords.

Betterbuy[10] give examples of the time it might take a hacker to crack a password:

Password	Time to crack in 2018
charity	0.22 milliseconds
Charity	18 hours 58 minutes 27 seconds
Charity1	5 months 2 weeks 3 days
CharityNo1	1 millennia 7 century 6 decades
!Charity98!	8414 millennia 5 decades 7 years
!Charity98!No1	Infinity

[10] https://www.betterbuys.com/estimating-password-cracking-times/

Defending your charity from password attacks

Building rules for your charity will help prevent successful password attacks.

- Avoid single dictionary words that can be easily guessed or information that might be apparent via social media such as family or pet names
- Use a string of random words rather than one long word or complex combination that might be difficult to remember, for example 'salttrainfish'
- Consider using a password manager to store all complex passwords, use a reputable product and make sure that it is protected by a strong password. This ensures that you only have to remember one password.

Advanced authentication

To combat password cracking, charities can implement various different defences. Consider using two-factor authentication to protect your charity's most sensitive information.

6. Humans

Charities in particular may have an increased risk of human error causing a cyber attack or a data breach.

This is due to the higher than usual turnover of temporary employees and volunteers working for charities. Those who have less experience with procedures and regulation have more potential to let in a threat.

The insider

The insider may be a disgruntled employee intentionally trying to attack your system or just someone who unintentionally enables an attack.

The trouble with humans

Humans, being humans, are prone to making mistakes. For data breaches, this could be as simple as emailing the wrong person or leaving a tablet or smartphone on the bus.

In terms of cyber attacks, inexperienced employees and volunteers are likely to be more susceptible to responding to a phishing scam as they may find it harder to recognise the warning signs.

Equally, charity staff and volunteers are often predisposed to be helpful. They may be less suspicious and, in a sense, too quick to help.

How to help your humans

Building an internet policy for your charity means you have set rules and protocols that everyone in the organisation can follow.

What is an internet policy?

An internet policy describes your charity's privacy and data security rules. It should be shared with all new starters and kept as a point of reference. It might include day-to-day responsibilities your employees should adopt, such as:

- Use password or PIN protection for all tablets, smartphones and removable storage devices such as USBs
- Log off computers at the end of the day and lock them away
- Learn the types of information which are sensitive or confidential
- Understand what their responsibilities are with regards to protecting the charity's data
- Monitor temporary employees and volunteers ensuring they know and understand the policy too.

The policy can be shared with all new starters as a form of written conduct they must sign up to.

In addition, training should be provided on how to handle data appropriately both on and offline, including how and when to encrypt data.

The following page gives an overview of the considerations which employees should make with regards to how they protect data in a variety of situations.

How your charity can protect against data breaches

Cyber security plans should be thorough and consider all data held by your charity, not just that which is in use.

Only keep data the charity will use

Minimise the number of places the charity stores personal data and reduce the volume of information you collect. If you only retain what is necessary, you minimise the opportunity of risks occurring.

Safeguard data

- ✓ Lock away physical records containing any private information in a secure location
- ✓ Restrict employee access to private records to individuals with dedicated access
- ✓ Conduct employee and volunteer background checks
- ✓ Never give temporary employees, volunteers or third party vendors access to personal employee or customer information.

Clearing out old files

Be mindful of the private information held offline. Physical records may be disposed of over time as alternative storage systems become more convenient. To safeguard records your charity no longer needs, it's important to dispose of them safely.

- Cross-cut shred paper files
- Destroy disks, CDs/DVDs and other portable media so they are unusable.
- Before disposing of a hard drive; use software specifically designed to permanently wipe it clean (or physically destroy the drive itself).

Restrict system use to charity activity

Restrict employee and volunteer usage of computers and portable devices such as tablets to charity activities only. Avoid file sharing on peer-to-peer websites or software applications, block access to inappropriate websites and prohibit the use of unapproved software on all devices. Login accounts should be personal, not shared, and you should be able to control access so staff members can only interact with the data they need.

Manage the charity's use of portable media

Only allow encrypted data to be downloaded to portable storage devices. This provides effective protection against unauthorised or unlawful processing, especially if the device is lost or stolen. Restricting the use of physical ports (such as USB ports) can also improve security.

Breaches due to tele-matching - RSPCA

Data tele-matching describes a situation when a donor chooses not to provide information but the charity finds another way to enrich their data, essentially filling in the gaps.

For example, the RSPCA hired a company to enrich their data. They had been sharing data for many years and would use a phone number they had on record to find a current postal address. This was reported by ICO as a breach and the RSPCA have since stopped this practice.

The consequences of a cyber attack

Just over 70% of charities in our survey[11] claim they are fully prepared to deal with a cyber attack. Interestingly though, just over half have a cyber security plan in place.

After data breaches, the biggest impact charities identified as a concern following a cyber attack, was the cost of putting things right.

The cost of putting things right

Over 20% of respondents in our survey were unaware of the new General Data Protection Regulation (GDPR) in force from the 25 May 2018 but it spells significant changes for the way charities will need to respond to a breach [11].

The GDPR includes a requirement to notify the Information Commissioners Office (ICO) within 72 hours following a breach that puts personal data at risk. As well as that, there is also a requirement to notify individuals if there is a high-risk breach, for example if medical records were unavailable for a long period due to a cyber attack.

But how will you know how many records were lost? How will your charity cope if you can't recover the data? What will you do if someone takes legal action against the charity?

The costs of addressing the impacts of a cyber attack can be significant and charities in this situation are likely to require technical support.

How much could a cyber attack cost your charity?

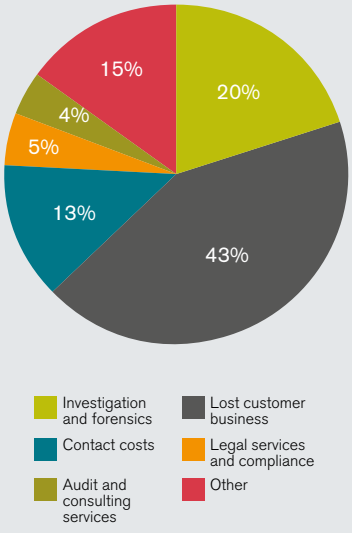
IBM Security and Ponemon Institute examined the costs incurred by 40 companies in 13 industries following the loss or theft of personal data.

They found the average cost per record for organisations in the UK to be £98 and the average for public sector organisations at an average of £59 per record.

Working off the average of £59 as an example, a charity that held 10,000 donor or service user records the cost would come out at a hefty £590,000.

The pie chart gives a breakdown of the factors which contribute to the overall cost of a data breach as a percentage. Though loss of customer data forms the largest proportion of this cost, the specialist services required to assist in charity's recovery are also a significant consideration.

Percentage cost of a data breach by category



Cyber insurance can help deal some of the consequences

This is why insurance can be a really important second line of defence. Not only will insurance help cover these costs, a comprehensive policy will support your charity's longer-term recovery with access to professional help.

Good to know

If you invest in cyber insurance, it's worth understanding what you're getting from the cover. Some policies may not provide cover for the financial loss resulting from cyber crime. Some policies might only provide cover for targeted attacks and not indiscriminate events that affect many victims.

We offer stand alone policies or cyber enhancements which can be added to your existing charity insurance. You can find out more information by speaking with your insurance broker.

[11] Ecclesiastical Annual Charity Tracking Survey 2017 by independent research agency FWD

Attacks on your reputation

A data breach is not the only impact a cyber attack can have. Following a cyber attack, a charity may experience bad press and a fall in public trust.

A charity's reputation is fragile. It can take years to build and only seconds to destroy. How the charity handles the cyber attack could make all the difference. In 2016, over 50% of all charities in our survey identified damage to individual reputations as their biggest concern in the wake of a cyber-attack, second only to the cost of breaching data regulations[12]. There are some cyber attacks which specifically seek to damage an organisation's reputation.

What is Hacktivism?

Hacktivism is used to describe cyber attacks with a political or social agenda. Hacktivist activity is usually disruptive in nature and could involve website defacement or a social media takeover.

Measuring the impact of cyber attacks on reputation

After TalkTalk suffered data breaches in 2015, Alva looked at publicly available comments and content such as social media posts, to assess sentiment towards the organisation. They were able to clearly show that with each data breach, public sentiment about the brand fell and by the third breach in one year, the impact is considerable. You can see Alva's findings represented in a graph of sentiment over time for the brand Talk Talk by following this link.

Contingency planning should cover responses to attacks and breaches.

Charities need to prepare with appropriate responses, issued according to tight timescales and demonstrating real empathy for those affected. Consider using a Public Relations firm to help you if you expect national media coverage.

A cyber risks contingency plan should address protocol in case of an attack including information like emergency telephone numbers and need-to-know contacts.

In response to concerns raised by charities last year, we adapted our charity insurance cover to help support you when dealing with risks to your reputation.

12 Ecclesiastical Annual Charity Tracking Survey 2016 by independent research agency FWD

Cyber insurance

Cyber insurance is also a way to manage cyber risks presented by hackers, ransomware and other threats.

It's important first and foremost that charities defend themselves by having cyber security controls in place. However, where they are still exposed, cyber insurance can provide additional support.

Cyber insurance from Ecclesiastical can be bought in conjunction with your charity insurance or as a separate stand-alone policy.

Helping your charity to cover the costs

Charity cyber insurance insures the financial impact of a cyber attack including elements of:

- Costs of dealing with data breaches
- Cost of legal defence from cyber liability claims
- Cost of professional IT and forensic services
- Cover for loss of income from a cyber event.

Legal fines and penalties issued to charities are not usually covered by insurance policies. However, legal defence and compensation awarded to third parties can be.

Support services and access to experts

Our cyber insurance policies offer additional services to help charity organisations manage the aftermath of an attack.

Professional services such as these can be expensive to use. Cyber insurance gives your charity access at **no additional cost:**

- PR and crisis helplines to help manage reputational risks following an attack
- IT and forensic investigation experts to recover lost files and secure the system

If you already have charity insurance with us, you will find some elements of a cyber attack are covered. A cyber-specific insurance policy will be more comprehensive and give extra support to help your charity recover.

Final thoughts

Defending against cyber risk is a common purpose for charities, charity sector bodies and, in fact, all individuals and organisations. As the challenges emerge and change we are continuing to learn together.

One of the key findings from the NCSC in their cyber threat assessment for the UK charity sector is that the scale of cyber activity against charities is unclear.

"Whilst some charities report cyber incidents externally, others may not for fear of reputational and/or financial consequences, or through uncertainty of how and where to register the offence. Under-reporting is hindering our understanding of the scale of the threat to the charity sector."

Charities need to support each other by sharing their experiences and solutions to build a 'cyber safe' future for the sector.

The Charities Security Forum website and blog provide helpful information in relation to cyber risk to charities. They include examples and experiences from charities and we have included some other helpful links where you can find advice and support.

> Cyber risks are ever-evolving and we're proud to have produced this guide to help charities evolve their defences. While insurance is not the only solution, cyber-cover can be a vital part of any cyber security plan. The policy not only covers the costs following a breach or cyber attack, but importantly it gives access to experts to support charities in dealing with cyber risk and the aftermath of an attack or breach. We believe that through a combination of awareness, careful risk management and insurance solutions, we can help support a safe future for charities and their digital operations.
>
> **David Britton, Charity Director**

Helpful links

What to do if you're suffering a live cyber attack

Tips and advice from ActionFraud on how to deal with a cyber attack as it's happening, including their 24-hour support helpline.

ICO data breach notification

Following a cyber attack, your charity should notify The Information Commissioner's Office as soon as possible.

Common cyber attacks and reducing their impact

A white paper on reducing the impact of common cyber attacks from the National Cyber Security Centre.

NCSC Cyber Security Small Charity Guide

How to improve cyber security within your organisation – quickly, easily and at low cost.

An overview of GDPR from ICO

Any digital strategy created now should implement GDPR regulation to protect data. The Information Commissioner's Office have given a helpful overview of the new regulation.

Cyber Essentials scheme

Helpful tips on cyber security described in plain English.

IT Induction and Information Security Awareness

A pocket guide that puts forward the case for an organisation-wide, and fully supported IT Induction and Information Security Awareness Programme.

The IASME Consortium

An Accreditation Body for assessing and certifying against the Government's Cyber Essentials Scheme.

Charities Security Forum

A group of information security people working for charities and not-for-profits, addressing the security problems affecting the third sector.