Cyber threats explained

UK CHARITY SECTOR

ecclesiastical

Contains promotional material

Cyber threats

Introduction

The UK has a thriving charity sector and generates an annual income of over £90 billion, which is over 50% larger than Tesco's annual sales, the UK's largest supermarket chain. This makes the charity sector a major target and their assets and reputation are at risk. Whilst most people would find it unconscionable to steal from a charity, there are a growing number of cyber criminals looking for financial gain.

Larger charities may be able to protect themselves from attacks. However, smaller ones may feel that they fall below the radar of cyber criminals and are not targets. As smaller charities may not perceives themselves at risk, it's less likely that they will divert more of their limited resources away from fundraising to cyber security.

In today's digital world, charities have an increasing reliance on IT and technology for fundraising, streamlining operations and raising awareness. As a result, the cyber threat has become an unavoidable cost of being a charity in today's world.

Charities have an open and trusting nature and trust that people who get in touch are looking to offer help and support. This level of trust can open up charities to attack from phishing emails that use 'social engineering' to trick people into giving up information, transferring money or downloading malware.

Many cyber attacks use indiscriminate scatter-gun approaches to target victims. If you're a charity, you're just as likely to be a victim of these scatter-gun attacks as a large organisation. Attackers may not know (or care) who you are until they get into your system.

Charities may not always fall victim to a direct attack. Charities, especially the smaller ones, often outsource responsibility for services such as IT and data to specialist companies. They may also share data with external organisations such as marketing companies. As a result, it may be possible to access the charity's networks and/or information through these suppliers. Additionally, cyber criminals may be able to access UK-based charity data through connections in other countries where the security may be less stringent than in the UK.

Recent Government Statistics[1], showed that a fifth of charities have suffered some form of cyber attack and among these charities that have identified an attack, **39%** identified at least one attack per month.

According to a survey by the Ponemon Institute[2], **72%** of hackers are opportunistic and **69%** of hackers would quit an attack if a organisation's defences were discovered to be strong. However, the majority of charities cannot deploy a sophisticated level of protection or resources like some private sector businesses, and sometimes the work undertaken is provided on a voluntary basis.

A cyber security breach can damage a charity in many ways ranging from disruption and data loss, damage through loss of intellectual property, denial of access to websites and services, physical loss or damage through viruses, ransomware and other forms of malicious software. The UK media now regularly feature stories about cyber attacks and they will be quick to report on a charity that may have been the victim of a cyber incident. This adverse publicity can significantly impact the reputation of the charity and discourage potential donors.

Legislation such as the Data Protection Act 1998, and the European General Data Protection Regulation (GDPR) which came into force in May 2018, can impose penalties on organisations for not taking appropriate steps to secure or prevent access to data about individuals.

According to the latest update from the UK's Information Commissioners Office (ICO)[3], charities reported 123 data security incidents in the first quarter of 2019-20 which equates to 4% of all data breaches in the same period. Whilst the introduction of GDPR has resulted in an increase in reporting, it is clear that the cyber threat is a growing and the charity sector is not exempt.

1. Department for Digital, Culture, Media & Sport 2019 Cyber Security Breaches Survey 2019
2. https://www.paloaltonetworks.com/content/dam/creative-assets/campaigns/corporate/ponemon-report/web-assets/PAN_Ponemon_Report.pdf
3. https://ico.org.uk/action-weve-taken/data-security-incident-trends/

Cyber crime

Cyber crime has now overtaken physical crimes such as burglary or robbery. Cyber criminals are highly organised and are finding a myriad of new and more sophisticated techniques to access data and information for the purpose of financial gain and to commit fraud. This can result in money being taken from a bank account or credit arrangements (such as loans or overdrafts) being arranged in your charity's name for the benefit of a fraudster.

There is also an increasing risk of the use of 'Ransomware' where an attempt is made to extort money from you by preventing access to your computer system or files until a ransom is paid.

Threat sources

Cyber criminals

Career cyber criminals are professionals who "work" in the digital shadows, and may well have made the jump from traditional crime into cyber-enabled fraud, using technology instead to lower the chances of getting caught.

The cyber criminal is motivated by one thing: money – and the more of it they can get their hands on, the better. Datasets containing personal details and financial information are an attractive target: such information will be sold in online criminal forums to enable fraudulent activity using those details. Charity datasets may contain personally identifiable information (PII) of donors, trustees, patrons, partners, paid staff and volunteers. Some large charities hold several million donor records. The data may also include payment details relating to donations including card details.

Cybercrime as a Service (CaaS) is the creation and sale of the tools of cyber crime by third parties to criminals and has boomed over the last few years. There are also well established marketplaces that provide specialist cyber crime skills for organised criminals.

Right now, cyber criminals are all about mass phishing campaigns. They are low cost, easy to pull off, and promise a good return on investment. Spear phishing is still a big concern, and it's much harder to defend against, but for value nothing beats a good mass phish.

Typically these campaigns are used to deliver malware payloads (often Ransomware), and the emails usually include a strong social engineering component.

Charities will continue to be targeted by cyber criminals and the level of sophistication used by the attacker will continue to increase. There's already evidence of convincing emails that use well crafted language that does not immediately put the recipient on alert unlike the 'Nigerian prince' scam which offers a big financial reward for very little effort but often features poor grammar.

The National Cyber Security Centre (NCSC, a part of GCHQ) consider it likely that cyber criminals pose the most serious threat to the charity sector.

Hacktivists

Wikipedia defines hacktivism as "the use of computers and computer networks to promote political ends, chiefly free speech, human rights, and information ethics". As with hacking, hacktivism can also be a force for good or evil.

With the use of social media, hacktivists can now spread the word and recruit across the globe with a single tweet or a Facebook post to carry out their agenda driven attack.

Hacktivists overwhelmingly favour attacking websites. Since its website is often the most publicly facing aspect of an organisation, this makes perfect sense. Their methods may include distributed denial of service (DDoS) attacks, website defacement, viruses and worms that spread protest messages; taking over social media accounts, and stealing and disclosing sensitive data.

In 2012, a Hacktivist using the name AnonVoldemort attacked a New Zealand-based charity's website, erased their data and left graffiti.

In the same year, The British Pregnancy Advisory Service (BPAS) had its website defaced by a member of the hacking collective Anonymous who claimed to have stolen about 10,000 records of website contacts and threatened to release them online. After an ICO investigation BPAS was fined £160,000 for failing to be sufficiently aware of the risks to its systems and data.

According to a study by Recorded Future[4], a global real-time cyber threat intelligence provider - the number of active hacktivist groups has more than halved since 2016, falling from 27 to just eight in 2018.

The NCSC believe that the charity sector is not a priority target for hacktivists, but even a limited website takedown or defacement, could have financial, operational or reputational implications.

Nation States

The Nation State hacker has a very high degree of technical expertise and sit at the top of the tree. They work for governments to disrupt or compromise other target governments, organisations or individuals to gain access to valuable data or intelligence, and can create incidents that have international significance.

They might be part of a cyber army or hackers for hire for companies that are aligned to the aims of a government or dictatorship.

The Nation State hacker knows exactly what they're getting into, and knows full well that the mayhem they are spreading overseas is tacitly supported by their state. They can work without fear of legal retribution and often have close links to the military, intelligence or state control apparatus of their country.

As some charities operate both in the UK and overseas and others play a role in helping formulate and deliver UK domestic and foreign policy. This could potentially make them an attractive target for states who oppose or mistrust their activity.

Script Kiddies

A script kiddie or 'skiddie' are the most common breed of hacker. Essentially bored teenagers or younger with, possibly, some programming skill who mainly use programs developed by other, more experienced, hackers. These amateur hackers attack for fun and seek recognition amongst their peers. They tend to be un-targeted in their approach, finding thrills in bringing down any system.

Script kiddies have youth on their side. If caught, they're unlikely to get more than a slap on the wrist for their actions.

4. https://tech.newstatesman.com/security/hacktivist-groups

Script kiddies are influenced by others such as organised crime gangs, who may manipulate or recruit them to do their dirty work. They can be used as a diversionary tactic by criminals, creating a smokescreen of small, obvious attacks to mislead or distract investigators.

The tools they use vary, with many freely available and downloaded from the internet that are either used indiscriminately or as part of sophisticated, targeted attacks aimed at achieving specific goals. Given the abundance of hacking tools online and easy access to information, script kiddies are the largest threat by number and growing.

Cyber Terrorists

These groups such as Daesh (ISIS), Al Qaeda and affiliates, generally motivated by religious or political beliefs, attempt to create fear and chaos by disrupting critical infrastructures. Whilst this group has big ambitions, to date, there have been no publicly reported cases of terrorists using the internet to carry out cyber attacks; what has been done that has been attributed to cyber terrorism is more akin to hacktivism such as website defacement.

Insiders

The insider comes in both accidental and malicious forms: the disgruntled staff, the well-meaning innocent, or the supplier with trusted access to the charity's network. The insider may conduct their activities on purpose, through carelessness, or through outside influence falling for a scam or becoming the victim of blackmail, for example.

This makes the insider one of the hardest threats to anticipate and defend against. The insider's position within an organisation can mean they can do just as much damage as the most sophisticated piece of malware. Whatever their motivation, the insider possesses access to the charity's systems, and the means to breach or bypass defences with ease.

Alternatively, an insider may simply be a well-meaning individual trying to help what they think is a parent, contractor, colleague or student out.

In 2017, Simon Price, former chief executive of Birmingham Dogs Home, was sentenced to 5 years in prison in for stealing over £900,000 from the charity. Price was able to authorise payments to his personal bank accounts using a combination of fraudulent invoices from marketing firms, construction companies and solicitors.

Threat actions

The threat to the charity sector is varied and ranges from high volume, automated and opportunistic attacks to highly sophisticated and targeted attacks involving bespoke malware.

Malware

Malware (or malware software) is the term used for software that can be used to compromise computer functions, steal data or otherwise cause harm to the a computer. Malware is a broad term that refers to a variety of malicious programs.

Most malware requires user error or in-action to make it onto a computer system. Usually, hackers will try a variety of tricks to get victims to download, install, and run malware on their computers or devices. Malware distribution is largely dependent on social engineering for this purpose.

Common types of malware

In 2018 AVTest, an independent IT security institute recorded that 856.6 million types of malicious software (malware) have been created. In 2010, this figure was only 47 million which shows an 1800% increase in only 8 years. New variants such as the 2017 WannaCry attack which infected more than 300,000 computers around the world including numerous NHS trusts in the UK demonstrated that malware can still be extremely successful.

Virus

Just like a biological virus a computer virus has similar traits. Viruses pass from one computer to another. Like biological viruses, they can't reproduce on their own and need a host i.e. a program or document. Viruses must be activated by the user in order to cause trouble.

Trojan Horse

A Trojan Horse or Trojan, takes its name from the famous wooden horse and operates in a similar way. Trojans are installed on a victims machine through deception and would appear to be a file or document. They then spring into action and can delete files, destroy information or allow outsiders to access the computer.

Spyware

Spyware includes any type of program that spies on a person's computer activities. It may gather personal information such as usernames and password or account numbers. It may also track any websites that you might visit or emails you send and receive.

Worms

Worms are standalone programs that are often disguised as an attachment and are installed once it's opened. The worm can spread in many ways and can travel from one computer to another without any human interaction. Once activated, worms can open up remote access for hackers or enable the computer to be used in a denial of service attack (DoS).

Ransomware

Ransomware is an aggressive form of computer malware that is designed for direct revenue generation. The most common type today is crypto ransomware, which aims to encrypt data and files. The other, known as locker ransomware, is designed to lock the computer, preventing victims from using it and it then demands a ransom for their release.

The technology driving ransomware is increasingly advanced and uses 'zero day' flaws that may not be in the public domain, so can difficult to detect by many anti-virus programs currently in use today. The criminals either go for volume to infect as many victims as possible or they zero in on the human element, relying on tricking staff into interacting with an innocuous looking email, file or web link. Even with regular training, it only takes a single momentary lapse in judgement from a user to result in an infection.

Late in 2016, the British & Foreign Bible Society was a victim of a large ransomware attack, in which the personal data of 417,000 people was stolen. The attack lead to some supporter's payment cards and bank account details being at risk. The ICO fined the charity £100,000 for its poor cyber security measures, including an easy-to-guess password.

In 2016, Comic Relief's internal systems were down for several days after suffering a ransomware attack. As a result of the attack, staff at Comic Relief were unable to access their email or the internet forcing a number to work at home instead.

In July 2019, St John Ambulance was hit by a ransomware attack. Thankfully the attack was dealt with within 30 minutes and did not affect operational systems. The first-aid charity said it was confident that the attack, which targeted its course booking system, had not resulted in the theft of any data.

Some newer forms of ransomware rather than just encrypt the files also threatens to leak them online.

Research from the cyber security company Symantec[5] shows that ransomware attacks worldwide increased by 36% in 2017 — with more than 100 new malware families introduced by hackers and cyber criminals are increasingly targeting charities that have poor cyber defences.

5. Symantec Internet Security Threat Report. Vol 22. April 2017. (https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf)

How is malware distributed?

Email attachments

Malware is often disguised as innocent email attachments in phishing emails. Users are tricked into downloading software that poses as an invoice, form, image, or other document. Once on the user's computer, the malware either unpacks itself or waits for the user to attempt to open it before executing its code.

Microsoft Office formats such as Word, PowerPoint and Excel make up the most prevalent group of malicious file extensions at **38%** of the total. According to cyber security company Norton, in 2018 **71%** of all targeted attacks started with spear phishing[6].

Web links

Other techniques include directing victims to web sites under the pretence of a threat e.g. "*suspicious activity has been detected on this account*". These links typically lead to malicious sites that host 'Exploit Kits' which download malware onto computer when the page is loaded.

Storage devices

Some hackers leave malware-infected USB flash drives or other storage devices in public locations where they're likely to be discovered. When someone plugs the storage device into a computer to determine its contents, malware in the device can transfer itself to the computer and infect it.

Denial-of-Service (DoS) attacks

"Denial of service" or "DoS" describes the aim of this class of cyber attack that's designed to render a service inaccessible. The common type of DoS attack are those that are launched against websites. When a website suffers a DoS attack, the apparent effect will depend on its use. For the average user, it appears that the site has simply stopped displaying content. For others, it could mean that the online systems they depend upon has ceased to respond.

DoS attacks can range in duration and may target more than one site at a time. An attack becomes a 'distributed denial of service', referred to as "DDoS", when it comes from multiple computers instead of just one.

Sequel injection attack

A sequel injection, also known as SQL injection or SQLi, refers to a weakness that may allow hackers to steal or tamper with a database sitting behind a web application. This is achieved by sending malicious SQL commands to the database server, typically by inputting code into forms – like login or registration pages. SQL injection is the most common form of web site attack, often common web forms are not coded properly and the hacking tools used to find weaknesses and take advantage of them are commonly available to be downloaded online.

6. Symantec Internet Security Threat report, Vol 23. March 2018. https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

Phone fraud

Phone or PBX fraud (Private Branch Exchange is a private telephone network) entails external hackers taking over control of the charity telephone system, routing international or premium calls through it. The losses involved can be high, especially when they are made during times that a charity may be closed, for example the summer holidays. During this period it is likely that the fraudulent calls will go un-noticed until the telephone bill arrives.

In 2013. the National Fraud Intelligence Bureau (NFIB) issued a warning to UK small to medium sized businesses of the increase in PBX fraud. The NFIB has also noticed that a number of charities, schools and medical practices were being targeted by the fraudsters who are taking advantage of security flaws.

Nobody is immune, even the Police. When Scotland Yard's switchboard was compromised, the bill was £620,000!

Personal BYOD (Bring Your Own Device)

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 and 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.

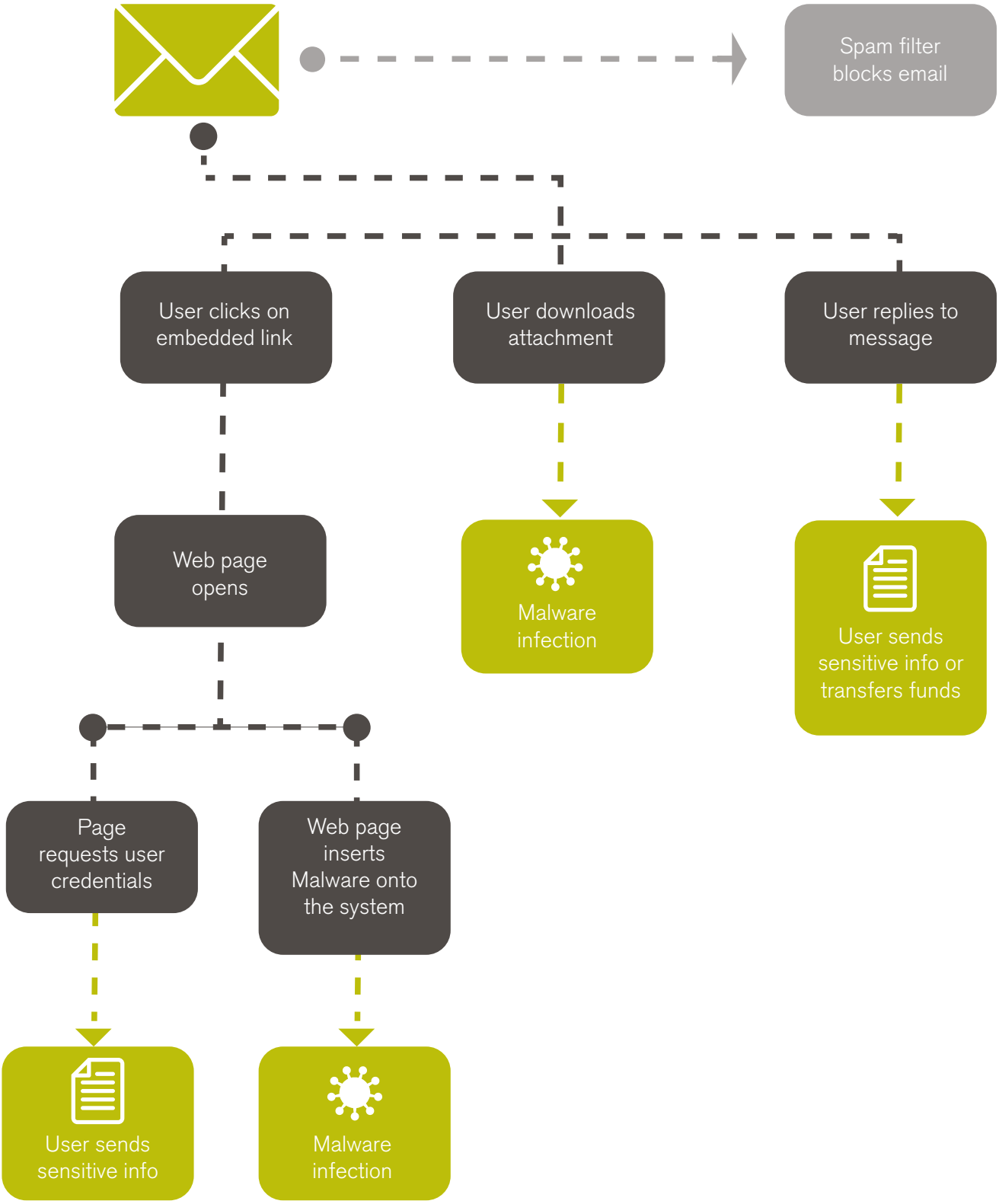
Charities are vulnerable to data theft, especially if staff or volunteers are using unsecure mobile devices to share or access charity data. As more small charities make use of BYOD technology, internal networks could be at risk from unsecured devices carrying malicious applications which could bypass security and access the network.

Phishing and spear phishing attacks (social engineering)

Phishing is an exploit that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they need or want. It is the simplest kind of cyber attack and, at the same time, the most dangerous and effective. Spear phishing is a targeted attack unlike traditional phishing which is indiscriminate.

In the three months after the introduction of the GDPR, the ICO, who are the regulator received an average of 500 calls a week to their breach reporting line. Collected data has identified that 50% of these related to phishing attacks. Malware (10%) and Ransomware (6%) were also other notable causes of breaches reported.

How a phishing attack works




2345
ALT

Email fraud

Cyber enabled fraud aimed at tricking employees with financial authority into transferring money to criminals is increasing.

Invoice scams are a serious threat to charities of all sizes and represent one of the fastest growing, lowest cost, highest return cyber crime operations. A cyber criminal will impersonate a trusted person and attempts too coerce a staff member to transfer funds to the phisher's account or divulge sensitive information.

For example, a charity refurbishing a property or undertaking works may be contacted by someone pretending to be their contractor. They might suggest that there's been a change in bank details or promise a discount for early payment.

Cyber criminals may succeed in prompting money transfers using purely social engineering, but more developed campaigns combine the fraud with the deployment of malware to capture information that can be used to generate greater returns.

The US outpost of Save the Children, revealed that an attacker managed to access an employee's email account and from there sent fake invoices and other documents designed to trick the charity into sending the money. The hacker pretended the money was needed to pay for solar panels for a health centre in Pakistan. It was a well-researched ruse as the charity had a base there for decades. By the time the charity realised that it was fraud, almost £800,000 had already been deposited in a Japanese bank account. Save the Children managed to recover most of the money thanks to its insurance policy.

In July 2019, a charity in Manchester became the victim of an email/bank scam where payment of almost £100,000 was transferred to the incorrect bank account.

The organisation was undergoing an extension to their centre and had been paying their invoices by BACS transfer for several months. A copy of a valid invoice and a request for change of bank details (on the building company's letterhead) was received via email.

At this point, the organisation's finance manager was on holiday and did not respond to the email straight away. Upon their return, they received a call chasing the payment and checking that the bank details had been changed.

The caller provided a legitimate excuse, explaining that the details needed to be changed due to fraudulent activity on the previous account. The finance manager replied that they had already paid the invoice for that period but confirmed they would update the bank details in preparation for the next payment.

When the next valid invoice was received, the funds were transferred to the new account as requested. It wasn't until the real building contractors began chasing for payment that the scam was revealed. It was a simple mistake but it resulted in a significant cost to the organisation.

According to their size and resources, charities have departments and/or individuals with authority or responsibility for transferring funds. Again, the culture of trust in the sector may make charities especially vulnerable to this type of exploitation.

In 2018, The Charity Commission warned charities to be vigilant to the rise in fraudulent emails aimed at charity finance departments, impersonating Chief Executives.

Password attacks

Password attacks refer to various measures used to discover computer passwords. This is usually accomplished by recovering passwords from data stored in, or transported from, a computer system. Password attacks are performed in several different ways and some of the most common are as follows:

- Brute Force attack

  If a charity publishes staff names, then a hacker can easily guess usernames and they can guess passwords locally or remotely using either a manual or automated approach. Password guessing isn't always as difficult as you'd expect. Most networks aren't configured to require long and complex passwords, and an attacker needs to find only one weak password to gain access to a charity's network.

- Dictionary attack

  A hacker uses a program or script to try to login by cycling through combinations of common words. In contrast with a brute force attack, where a large proportion key space is searched systematically, a dictionary attack tries only those possibilities which are most likely to succeed, typically derived from a list of words for example a dictionary (hence the phrase dictionary attack). Generally, dictionary attacks succeed because many people have a tendency to choose passwords which are short (7 characters or fewer), such as single words found in dictionaries or simple, easily predicted variations on words, such as changing a digit at the end.

Even common desktop computers are capable of running several billion passwords per second.

- Key logger attack

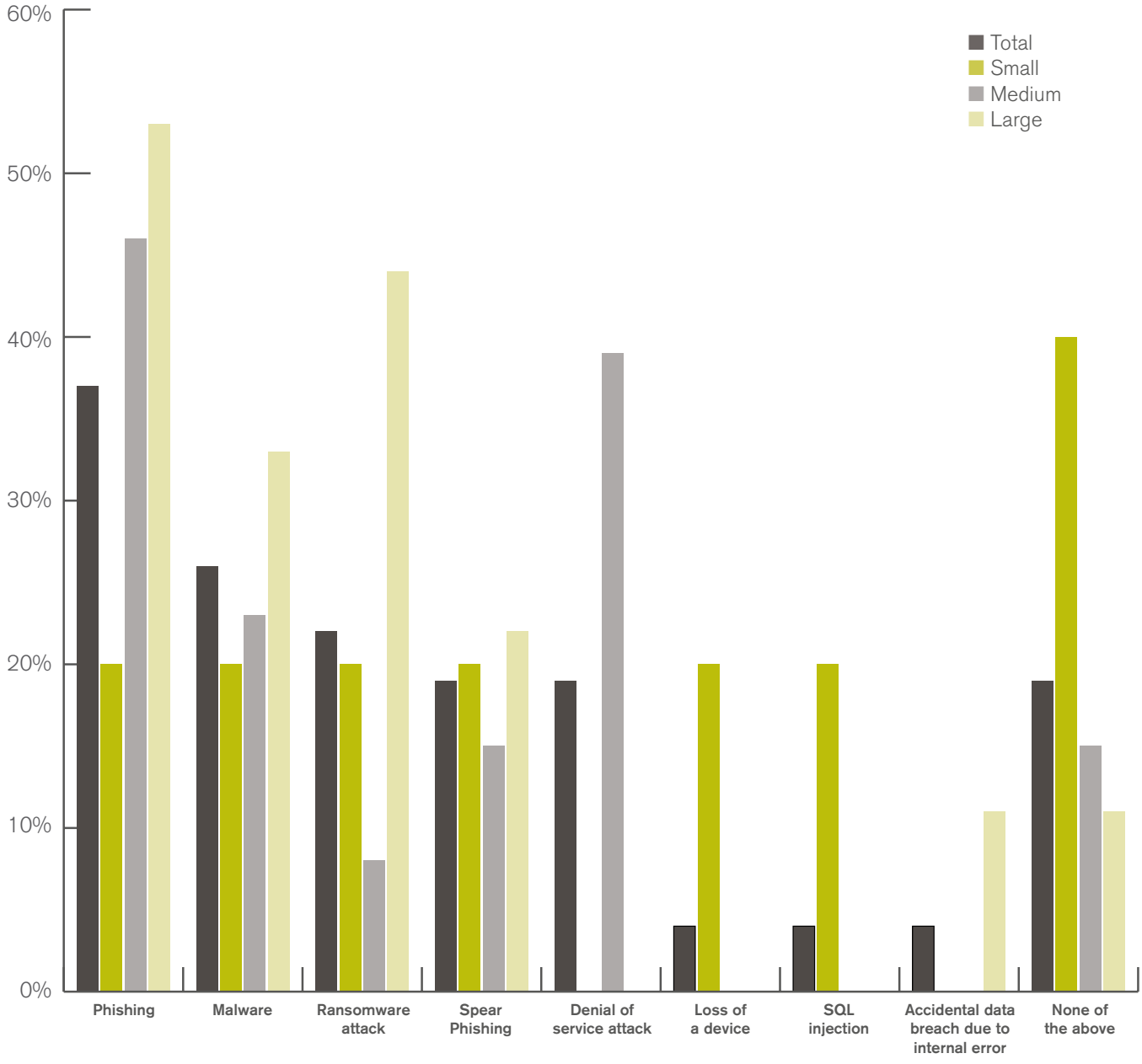
  Many attackers capture passwords simply by installing a keyboard-sniffing Trojan horse or one of the many physical keyboard-logging hardware devices for sale on the internet. Symantec reports that 82% of the most commonly used malware programs steal confidential information[7]. Most steal passwords. For less than £50, anyone can buy a keyboard keystroke logger that can log more than million keystrokes. Physical keyboard logging devices less than an inch long can easily be slipped between the keyboard cord and the computer's keyboard port. It's even possible to sniff passwords from wireless keyboards even from outside the boundary of the charity.

7. Symantec Internet Security Threat Report, Vol 23. March 2018 https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

Ecclesiastical's 2019 charity cyber study?

Charities have experienced various types of cyber-attacks, the most common is Phishing followed by Malware and Ransomware. Larger charities are more likely to have experienced Phishing. Small charities are the most likely not to have experienced any of these types of attacks.

Which of the following has your charity experienced?



Base: Those who have ever experienced a cyber-attach or breach. 27 respondents
Source: Ecclesiastical Charity Cyber Survey 2019, carried out by FWD

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

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.

PD4221 1 03/22