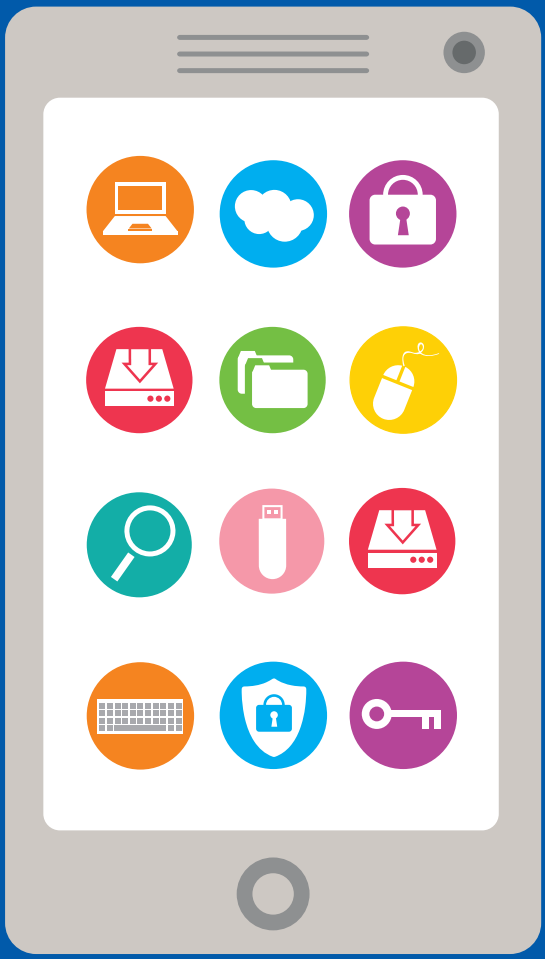
ZURICH



Understanding the impact of cyber and information risk

Contents

Introduction

As a journalist it's impossible to ignore the issue of cyber risk. Not just because we have a duty to protect information about our sources and readers, but because the issue has never been higher on the news agenda.

The latest in a string of cyber security stories came this April, when the internet was buzzing with news of the Heartbleed virus – a security flaw that put tens of millions of devices and personal information at risk.

High profile news stories such as revelations about NSA surveillance and the Heartbleed virus have contributed to greater public debate and awareness about data and digital security, and show that cyber security is a shared responsibility – not just just for those working in tech. It matters for the media, business and, of course, charities too.

As part of an ongoing partnership, the Guardian Voluntary Sector Network and Zurich Insurance have compiled this guide to provide charities with the advice, techniques and case studies they need to defend their organisations and employees against cyber risks.

It explores what charities can do to protect their data, staff and service users from cyber issues such as malware, phishing scams, email attacks and beyond.

If you would like to share your experiences, ideas and advice about how your charity is tackling the issues in this guide, please get in touch: kerry.eustice@theguardian.com

Kerry Eustice,
Head of Education and Society Networks,
the Guardian

theguardian
voluntary sector network

New technology, new risks

"Each success only buys an admission ticket to a more difficult problem." Although Henry Kissinger made this comment way back in 1979, it is very relevant to the challenges that technology presents to us today.

There is no doubt that modern technology has brought huge benefits to the way charities work, not least in increasing staff productivity. Email, word processing and spreadsheets have created huge efficiency savings for our internal operations, while laptops, tablets, smartphones and wireless data transfer have allowed us to work wherever and whenever we need to.

It has also become much easier to build external relationships and deliver charitable objectives. Today, the internet and social media are vital means for communicating with beneficiaries, donors and stakeholders. Entire services can now be delivered online for a fraction of the cost. Online fundraising has established itself as a vital source of revenue and continues to grow.

However, with all of this comes increased risk. The ability to store reams of data on a small hard drive and to send information and data over large distances electronically, along with the portability of hardware such as laptops and smartphones all make it easier for information to fall into the wrong hands. And our reliance on technology means we can be stuck without it.

Cyber risks can sometimes seem like remote, intangible concepts. However, charities are unfortunately not immune from the threat of hackers, who are keen to exploit security flaws and access the data of beneficiaries or staff. Charities cannot be complacent about the prospect of digital data being given away or lost as a result of carelessness or a lack of security training. And most charities will already be aware of how operations can grind to a halt as soon as trusted systems and infrastructure become unavailable.

There remains a lack of awareness about the cyber threats we face and the solutions that are available. This is manifest in the fact that several charities have now received substantial fines from the Information Commissioner's Office (ICO), while others have been publicly reprimanded. Last year, a report by the ICO, based on its advisory visits to charities, identified numerous areas where charities need to improve (see page 6 for more on this).

This guide aims to provide clear and practical guidance on the cyber and information risks, tools and strategies charities need to consider. Charities should also get in touch with their insurance providers who can assist them with their individual needs. We are keen to hear how you progress in this area. Please share feedback with me at hannah.clark@uk.zurich.com

Hannah Clark,
Head of Charities and Social Organisations,
Zurich Insurance

ZURICH®

4

Protecting yourself against cyber risk

Hacking is a problem which gains a lot of media coverage, but when it comes to cyber risk, deliberate and malicious behaviour is actually only part of the problem. Cyber risk (which is sometimes known as information risk), can broadly be categorised into three themes: direct, malicious cyber attacks; accidental information loss or misuse, and physical system failures.

Malicious attacks

It is not often that a whole new breed of criminal is created, but the rise of the internet has done just that. With enterprising computer programmers now able to break into organisations' confidential records, hacking has become a major cyber risk. One recent victim was JPMorgan Chase & Co, which lost the details of 465,000 prepaid cash card users after hackers attacked its network.

Hacking is not the only form of deliberate attack. Malware such as worms, trojan horses, spyware and adware can all disrupt or slow down operations or cause loss of data. Meanwhile, denial of service attacks can bring organisations to a complete halt, usually by saturating computer systems with a large number of communication requests. Such threats are becoming increasingly subtle. "Advanced persistent threats" aim to stay in a system undetected, allowing data to be stolen over a prolonged period. Often these embed themselves via "spear phishing", where employees are fooled by an email that appears to be from a trusted contact.

Charities are not immune to these threats. In 2012 an anti-abortion hacker obtained personal details of thousands of clients of the British Pregnancy Advisory Service and threatened to publish them. The charity had not realised that its website was storing the names, addresses, dates of birth and telephone numbers of women who asked for its advice, and it was later fined £200,000 by the Information Commissioner's Office (ICO).

Accidental data loss or misuse

Accidental loss of data may not have the same sinister ring that hacking has, but it continues to be a major pitfall for organisations. Data stored on portable devices such as laptops and smartphones is at risk if it is not encrypted, physically secured or treated with care.

Charities have recently made mistakes in this area. Last year the Nursing and Midwifery Council was fined £150,000 after it lost three unencrypted DVDs containing confidential personal information. The DVDs were to be couriered to another location, but the package

arrived without the DVDs, and there was no evidence to suggest that the the package had been tampered with.

Other charities have had data stolen because they failed to protect it properly. Notably, the Alzheimer's Society was publicly reprimanded by the ICO after several laptops were taken from its Cardiff offices in 2010. The laptops contained personal details of 1,000 staff members, but had not been encrypted or physically locked up.

Data need not even be lost in order to breach regulations. A member of staff might mistakenly email personal data to the wrong person, or material might be published on a website which is libellous, plagiarised or in breach of copyright.

Physical system failures

A further class of risks relate not to deliberate sabotage or carelessness as such, but to the difficulties of maintaining a complex technology infrastructure. Charities have become hugely reliant on computers and technology in order to operate, and the loss of internal systems or of website functionality can mean beneficiaries do not receive the help they need or vital fundraising revenue is lost. Alternatively, IT systems failure or damage coupled with a lack of disaster recovery planning could mean vital data or software is erased, destroyed or distorted.

Prevention and planning

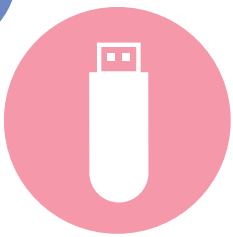
Firewalls, encryption and data backup provisions are obvious first steps in reducing cyber risk. However, it is a mistake to think that because we are dealing with technology risks, the answer is to simply fight them with more technology. In fact, effective prevention is as much about processes and education.

Strong business continuity planning is a vital platform for ensuring prevention measures are in place and for providing an action plan if a problem occurs. Defined triggers need to be in place so it is clear when a breach has occurred, as should control mechanisms, such as procedures to close down systems and communication plans. It also needs to include an escalation process, so that a breach progresses from employee to a manager and through the key communication channels.

All of this needs to be tested in practice. Business continuity testing of potential issues ensures that the plan can be modified if necessary, and that everyone is aware of what might happen and how to respond.

The importance of educating staff (see page 8) on the cyber risks they face and how to prevent them cannot be underestimated. We have heard about an organisation where a member of staff was given no training, and when an error alert repeatedly appeared on their screen, they simply kept on deleting it. The result was that 24-hours-worth of the organisation's data was lost. ➦

Responding to data loss



The first response to any sort of data loss, whether that loss be due to attack or an accident, is to consider who needs to be informed.

If a large number of people are affected or there are very serious consequences, the ICO will expect to be notified. It will want a description of how and when the breach occurred, what data was involved, what security measures were in place and what has been done in response. In cases of illegal activity, the police also need to be informed.

Perhaps most importantly, it is necessary to inform those whose data has been lost, and to do so in a timely and controlled manner – particularly when individuals may be able to protect themselves, such as by changing passwords or credit card pin numbers. Any communications should give clear advice on the steps people can take and what help the organisation in question can give them. It may also be necessary to inform the media to get these messages across.

Recent developments

Technology will continue to change the risk environment. For example, staff need to know that whatever they say on social media is public and accessible to the press.

The rise of portable hardware such as laptops and smartphones means "Bring Your Own Device" schemes are increasingly popular. While they offer great productivity benefits, such practices weaken the security of data, and it is necessary to have strong processes and protections in place.

Chris Greaves is Senior Strategic Risk Consultant at Zurich Insurance

LEARNING LESSONS

Awareness of cyber risk is increasing, and many charities are doing a good job of tackling it. However, there is more work to be done. Last year the ICO reported on advisory visits it had made to 32 charities, and revealed a number of areas that required improvement.

- In terms of technology, roughly half of the charities the ICO visited had failed to disable USB ports and DVD/CD drives on computers, leaving them open to the removal of data or uploading of malicious code.

- A significant proportion of these organisations also did not have minimum requirements for password complexity, nor did they enforce basic security principles, such as regular password changes.

- When it came to education, over a third did not have refresher training for staff who handle personal data. The ICO particularly highlighted the need for volunteers to receive regular training or awareness sessions.

Our experience is similar. Most charities are conscious of the cyber risks they face, but implementing the full range of controls and processes to ensure full protection is not always easy. Constructing a strong business continuity plan is the starting point for ensuring that all the bases are covered.

Case study: Never be complacent

A cyber and information risk strategy should continually be reviewed and adapted, says Ray Fletcher of Dimensions, a non-profit organisation that supports 3,500 people with learning disabilities and autism.

Working with Zurich Insurance, we recently embarked on a process to determine Dimension's points of risk, such as if there were any "open doors" we were unaware of. We found three main points of entry: our website; our remote desktop; and the mobile applications we develop to help staff do their jobs. We also discovered weaknesses within the web services that "talk" to the mobile apps, which meant it wouldn't have been impossible for an interrogating application to attack our systems.

Once we had established our vulnerabilities, we considered what protection we already had in place and what was needed to fill any gaps. This was about more than just passwords and anti-virus protection. It was about recognising what was talking to us at the other end. For example, did we know if it was one of our 5,000 staff members or someone else who was using an app at a particular time? We subsequently decided to limit the number of devices that could access our systems so we knew exactly who was in them at all times.

We then prioritised the risks we faced. By establishing which were the most dangerous and important we could act accordingly. For example, we have an in-house app that is used for scheduling staff visits to beneficiaries. We discovered it had a vulnerability that could enable hackers to see when and where visits were due to take place. This put the safety of our teams at risk so we had to turn this app off while we plugged the hole.

If not-for-profits and charities don't have a cyber and information risk strategy in place they should speak to their insurance company for help creating one. There are policies freely available on the internet but using these is risky in itself as you don't know who has written them, or for what purpose. You may inadvertently come across a policy written by someone who deliberately wants to weaken organisational systems.

All of our employees have training in data protection and we enforce strict security policies. However, the most important thing is that we are never complacent. Cyber risks change perpetually; as quickly as new security measures are introduced people find a way to get round them. We always need to be on the lookout for the next vulnerability.

Ray Fletcher is Head of IT at Dimensions

The power of learning

Educating employees about technology's common risks is a non-profit's most potent weapon against cyber crime.

There are, it is said, two kinds of organisations today. Those who have been hacked – and those who don't yet know they have been hacked. Recent attacks on vast corporations such as Target, a US retailer which in 2013 lost the credit card details of 40 million Americans in the biggest retail hack in history, have rung alarm bells about the ferocity of the cyber crimes we face. Such organisations have access to vast resources to protect them, both in terms of the technology and the skills they can deploy. Yet still, they failed. How then can smaller non-profit organisations – often with minimal budgets – defend themselves?

Certainly, there is technology available to help keep us safe. But education is our most potent weapon against cyber criminals and vandals. Developing the skills to recognise threats and stay secure must become part of everyone's job, particularly reflected by those at the top.

The situation we find ourselves in is not entirely novel. In the 1970s, factory safety was dreadful. The many accidents demonstrated a different approach was needed. Safer technology was often only a partial solution. A better option was to change the culture to one where you were not allowed to do your job if you couldn't do it safely. Education was at the heart of this sea change.

How can we achieve the same kind of impact in cyber security? The education we need is more than mere training. We need to teach people principles concerning how they conduct their work, as well as the technical knowledge needed to know what practices are hazardous. These principles will be different for every organisation, but at a basic level they might include: never clicking on links without knowing they are genuine, never using USB sticks at work, having clear rules about how home/work devices can be used, or making sure a manager knows when you suspect someone else is doing something unsafe. A poor safety culture affects us all.

How should this kind of education happen? Almost certainly, a combination of learning methods is most effective. Live sessions led by a group leader can help make a whole team more vigilant about new kinds of attacks. Online tutorials, such as those at theguardian.com/cyber-risk-tutorial, can help those who feel lost in new technology, and can show them how and why certain actions can leave the organisation at risk.

Above all else, remember that education comes from leaders. The best managers are the best teachers; they lead by example and set standards for the rest. For small organisations fighting to keep themselves safe, a small amount of education in these various forms can have an enormous impact on cyber safety – even without the budgets of the giant victims of the recent past.

Professor David Upton, Saïd Business School, Oxford University, is an expert in cyber-skills capacity building for companies and non-profits

Case study: Simplicity is key

Training staff in cyber security doesn't have to be complicated as long as you frame it in the right way.

A few years back, Alzheimer's Society was looking for a more formal system for classifying information because it was often difficult for workers to apply appropriate security controls when working with electronic files and paper documents. While the concept of protecting information has always been widely recognised and supported, a way to measure the risks was needed in order to manage them as effectively as possible. We had also recently been subjected to a theft of laptops which contained personal data and we wanted to make sure this type of incident never happened again.

The project team needed to define meaningful classification levels which could be understood and applied by all. In the many conversations about information security, a theme clearly emerged; the anecdotal example from past newspaper headlines of secret information left behind by a traveller on public transport. Clearly, this was a concept that was widely recognised and so it formed the basis of the classification framework, which became known as the "Left on a Train Test".

The test is a risk-based approach which develops from one question: If you had this information on a piece of paper which you left behind on a train and someone else found it, what could the consequences be?

Based on the potential impact of information being found on a train, one of three classification levels is assigned:

- Public – no impact or positive impact
- Internal – minor impact, inconvenience or embarrassment
- Confidential – moderate or major impact, violation of privacy, damage to reputation, financial loss

For each level there is a set of controls for handling the information in a number of formats and circumstances, which are used to manage the likelihood of the information risk.

The simplicity of the classification levels and the use of a familiar scenario allowed the system to be adopted without difficulty at all levels of the organisation. Many users of the classification system will not realise that they are applying a confidentiality-focused risk-based approach to information assurance with an associated matrix of format-specific controls; to them, it's just the "Left on a Train Test" - and it's working.

Rowenna Fielding is Information Governance Manager at Alzheimer's Society

Tips and techniques for staying safe

The number of cyber threats may be growing, but with the right tools any organisation can fight back.

Our march into the "cyber era" has no doubt brought obvious benefits. Yet, as we know, with new practices come new challenges. With a more visible and intricate online presence comes the risk of hacking or website failure. Employees are far more mobile than ever, with many moving information seamlessly between personal and work devices. Recent research from a Sony survey revealed that 90 per cent of people admitted accessing company data from a personal device.

So whether you're looking to expand your charity's online platforms or planning on inviting employees to use their laptops in the office, there are some basic security features that every organisation should be aware of.

Data protection

Protecting an individual's data is more than just a courtesy – it is upheld by law. The Data Protection Act 1998 requires organisations processing personal data to meet a number of legal obligations and register with the ICO. The main principles include requiring personal data be processed "fairly and lawfully", that data should not be kept "longer than is necessary for purpose" and that "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

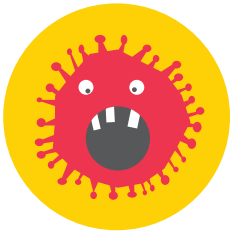
In the most serious of breaches the ICO can issue penalties of up to £500,000. Beyond fines though, a serious data breach can have an even bigger impact on organisation's hard-earned reputation and a long-lasting impact on their relationships with those they work with.

Encryption

Often, the go-to solution for keeping information safe is an encryption programme, which can be used to encode anything from messages and documents to personal details and passwords.

Encryption software uses mathematical algorithms to scramble data so it appears unintelligible to intruders. Encrypted files can be unlocked only with a "key code" held by the main user or those they wish to share the information with. This encryption and decryption process has historically been used by governments and the military, and is considered a simple and effective way to keep both standing and in-transit data safe.

Viruses and malware



Viruses are self-replicating malicious software that hamper a device's ability to function. Viruses can steal hardware space, access private information, corrupt data, spam contacts or log keystrokes when entering passwords. Having robust anti-virus software is therefore a must for any organisation.

Solutions to viruses and malware begin with an understanding of any device's two key components: hardware, which are the physical elements; and software, which are the "intangible" programmes such as email, internet browsers and word programmes that make a device so useful.

Software programmes are, in the main, more vulnerable to viruses and malware. Both organisations and individuals can protect themselves by embedding protection measures – such as a firewall – into the hardware of their device. The downside to hardware embedding, however, is that it can be more expensive and tricky to configure.

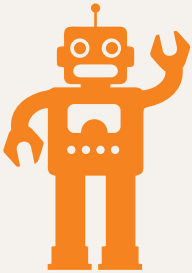
Passwords and anti-theft protection

A password or pin code is often the first line of defence between an information network and the outside world. From a user's point of view, it can be difficult to remember lots of passwords, which means many of us tend to use the same password for everything, which isn't very safe.

Passwords can be strengthened by unusual characters or by software that requests randomly generated pieces of the password rather than the whole thing. Meanwhile, anti-theft technology ensures a thief cannot get in even if they know your password. This technology has become increasingly clever. Stolen devices can now be told via SMS to "lock down" and cloak important data such as encryption keys, passwords, and other critical files. Some anti-theft technology can even be set to trigger if the device senses it is being tampered with.

LOOKING AHEAD

An increasing focus on user-friendly and adaptable solutions, such as Apple's new fingerprint login for iPhones, suggests a direction for the future of cyber security. Ultimately, as safety measures evolve to keep pace with, or even outpace threats, charities can take comfort in knowing that solutions are out there if they take the time to understand their needs, possible points of weakness, and the kind of options that are available to them.



Charlotte Simmonds is a freelance journalist

How not to get hacked – and what to do if you are

What picture does "hacker" paint in your mind? Most of us probably gravitate toward one of a lone, basement-dwelling cyber criminal surrounded by an army of computer monitors. In reality this image, while not entirely inaccurate, is only part of the picture.

A hacker is someone who seeks and exploits weaknesses in a computer system or computer network. Today's hacking jobs take many forms, whether carried out by professional networks, disgruntled individuals or petty criminals testing the boundaries. Even governments and multinational corporations have been accused of hacking websites for their own purposes. In 2011, for example, the French energy company EDF was fined £1.4m for gaining access to Greenpeace's computers where it was looking for sensitive information about the organisation's anti-nuclear energy campaign operations.

The urge for a clear definition of "hacking" may be tempting, but embracing a plurality of possibilities ensures an organisation will be prepared for anything. There are also a number of steps an organisation can take to minimise the likelihood of occurrence, or to reduce the damage should such a situation occur.

Prevention

Define your strategy. What is your charity's process for controlling information at both an overall and individual level? As Zurich's senior risk consultant Chris Greaves explains, this means thinking about how your public and private information is managed and what kinds of risks you are prepared to tolerate. Ask yourself: is our security strategy in keeping with our values?

Know your soft spots. Identifying chinks in the armour early can mean better protection down the line, says Greaves. He recommends assessing your current network and its perimeters, filters, and authorisations. How does information travel, and where does it go? Who has access to what? Pinpoint the areas of potential malicious attacks and then begin to fortify.

Tools and techniques such as those identified on page 10 and 11 can be a good place to start, but for more information charities can contact the Charity Security Forum. It provides support in the form of whitepapers and even mentoring for all UK-registered charities.

Understand the value of information. Charities deal with sensitive data every day, and this responsibility should never be taken lightly. Human nature dictates that prized items are treated with greater care, so think about the value of your data not just from a strategic or a financial perspective, but from a personal one too.

After the hacking

Communicate internally and share learning. Should an incident occur, it is important to sit down together and talk about what went wrong. Too often, an understanding of cyber threats and how to prevent them resides solely with the IT team. In-depth, open and active organisational learning should be encouraged as a priority.

One of the most important actions to take after a breach is to contact the Information Commissioner's Office. It can then provide your charity with additional help and advice. It has various rules that all organisations are required to follow, including that strategies are in place for dealing with such a breach. These strategies must include the following:

- a recovery plan, including damage limitation
- assessing the risks associated with the breach
- informing the right people and organisations that the breach has occurred
- reviewing your response and updating your information security

Incidents should be reported directly to the ICO in a timely fashion. A form for doing so is available to download at ico.org.uk/for_organisations/data_protection/lose

Take action. Immediately change the password on the affected service, and any others that use the same or similar password. There's also a possibility that the attacker got in via your machine as almost all malware is installed by victims themselves, if unknowingly. This is where a good anti-virus product is a must. Run a detailed scan and make sure you remove any viruses before starting a file recovery process.

If it is an email account that has been hacked, most providers will supply you with a way of getting your account back, which typically involves answering some identification questions. For more serious breaches, speak to the ICO for advice.

Often one account is a gateway to another, so it's important to check the hacker won't also be able to access other areas of your IT system. For example, your website might offer a direct route to your database or your bank account. Check they haven't also been compromised and change the passwords.

By taking the right steps to protect yourself, you can secure your organisation, and by knowing the warning signs to look out for, you can keep your personal details locked up tightly.

Gareth Jones is a freelance writer and editor

Content commissioned and edited by Slack Communications, on behalf of Zurich Insurance and Guardian News & Media.

Visit theguardian.com/zurich-guides to download an electronic version.

ZURICH®