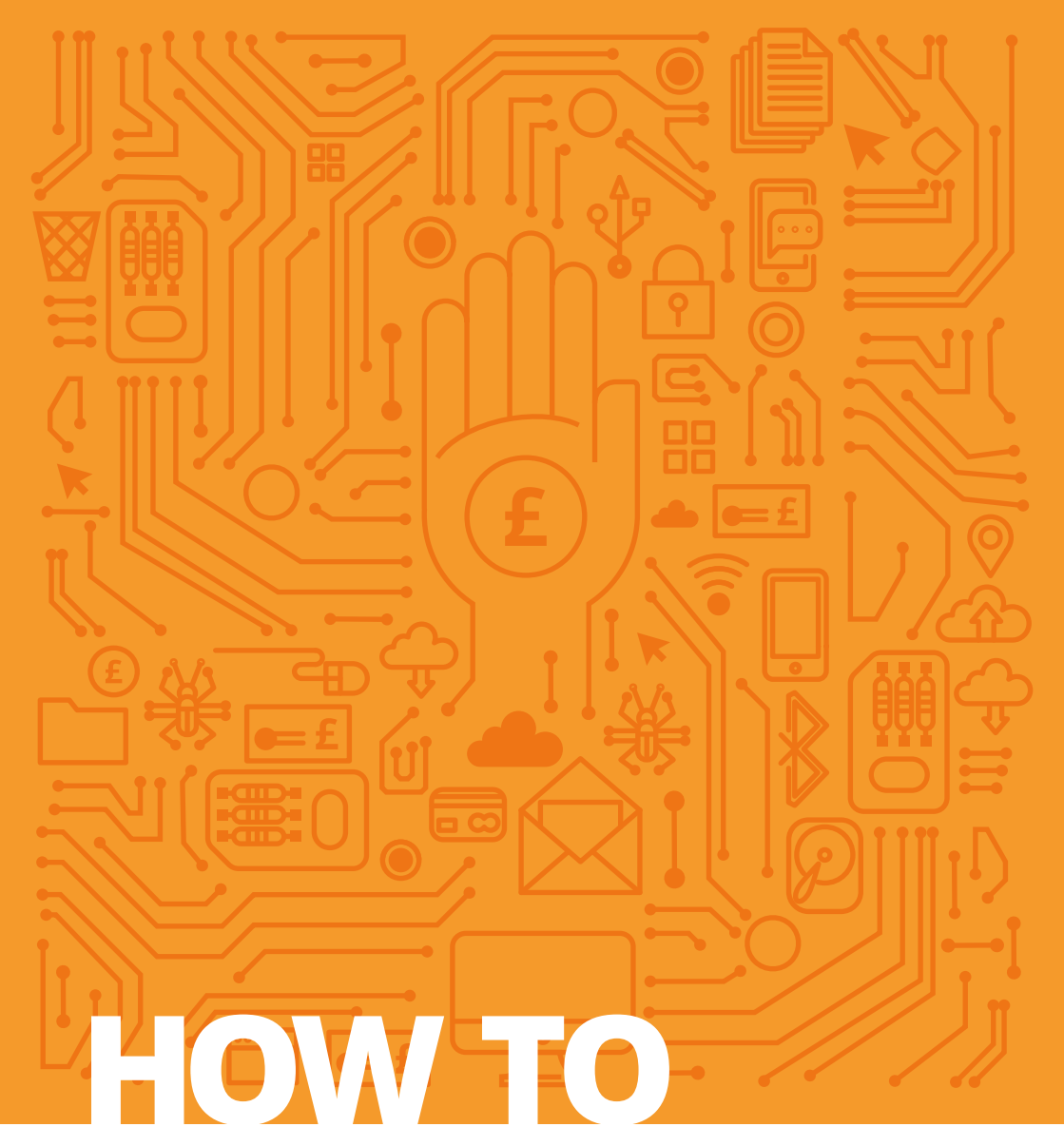


HOW TO

Protect Your Charity in an Evolving Digital World

A non-technical guide to the risks, threats and mitigations for charities.

itlab

“The single piece of advice I would offer other charities? It’s better to invest in security than spend money recovering from a cyber-attack.”

Mark Devis - Head of Technology, Christians Against Poverty

Table of Contents

Charities:
Rich Pickings and a Soft Target for Cyber Criminals?

Hackers see charities as a viable target; they are perceived to sit on cash and spend frugally on defence. By their nature, they are a treasure trove of personal information. Donors, volunteers and even vulnerable service users; all are ripe for identity theft.

While most charities view cybersecurity as important, competing demands - such as core service provision and fundraising – often mean that vital technical controls and staff awareness are not prioritised.

Sadly, recent research bears this picture out. In a significant survey* one third of UK charities disclosed that they had been breached in the last two years.

Dangerous Assumptions

The survey and other research highlights differing attitudes towards cybercrime. In common with the private sector, knowledge is growing. However, mistaken beliefs or a lack of knowledge in some charities places them in a vulnerable position:

- The 'it will never happen to us' mentality.
- Our charity is too small to be of interest to attackers.
- Not making the link between data protection and cybersecurity, conceptualising them as separate issues. Can be especially true of smaller charities.
- Focussing on monetary loss and not putting a price on being unable to operate.
- The belief that all necessary controls and defences are in place because IT is outsourced. This may not be the reality.
- Seeing cybersecurity as an unaffordable luxury.

Sometimes it takes a breach to spur a charity into action. As well as being an extremely painful way to learn, the costs recovering from an attack are often higher than the investment in good cyber hygiene and preventative measures.

* Cyber security among charities, August 2017, Department for Digital, Culture Media & Sport and Ipsos MORI.

Cybersecurity:
The Challenges and the Drivers

CHALLENGES

- Restricted budgets
- Culture of cost cuts
- Limited expertise in-house
- Lack of central office / HQ
- Remote working
- Competing priorities
- Low awareness
- IT outsourced (security at arm's length)
- No security champion
- Juggling multiple roles
- Part time IT personnel
- Personal devices
- Insecure legacy systems
- Lack of engagement among trustees (especially older demographics)

DRIVERS

- Stakeholder confidence
- Reputation and brand management
- Avoidance of fines (e.g. ICO)
- Safeguarding vulnerable service users
- Lower risk of data breaches
- Donor trust and loyalty
- Aids compliance with regulations (e.g. GDPR)
- Peace of mind
- Donor protection and confidentiality
- Reduced risk of monetary loss
- Continuity of care/service
- Meeting accreditation standards of commissioning organisations (e.g. local councils)
- Fosters confidence adopting new tech
- Potentially improves efficiency and user-experiences

In this guide, Michael Bateman, IT Lab's Director of Cyber Services, explains some common cyber risks and shares pragmatic advice on how charities can improve security. We hope the insights and tips prove useful, and will help you to manage your personal and organisational cyber threats.

“The cyber threat is real and growing, and the type of threats we face are always evolving.”

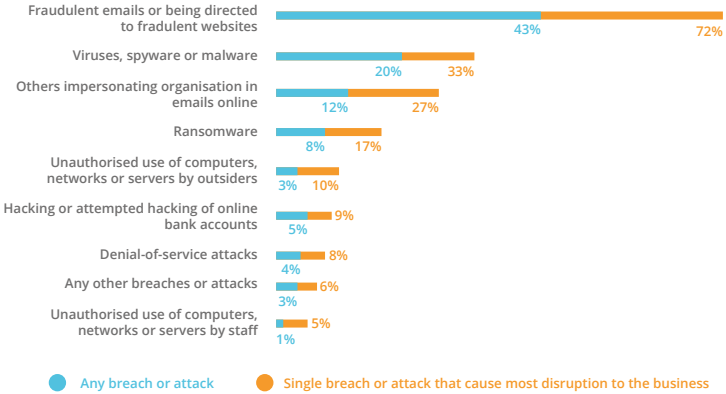
National Cyber Security Centre (NCSC) from annual review 2017

Charities face the same risks from cybercrime as any other sector. Cyber attacks are also on the rise. In its first year, the NCSC received 1,131 incident reports, with 590 classed as ‘significant’. An untold number go undetected or unreported.

In 2017, almost half of UK firms were hit by a cyber breach or attack, compared with one in five the previous year. In wider reaching research by the Department for Culture Media & Sport, Ipsos MORI and the University of Portsmouth, the results on the next page reveal that:

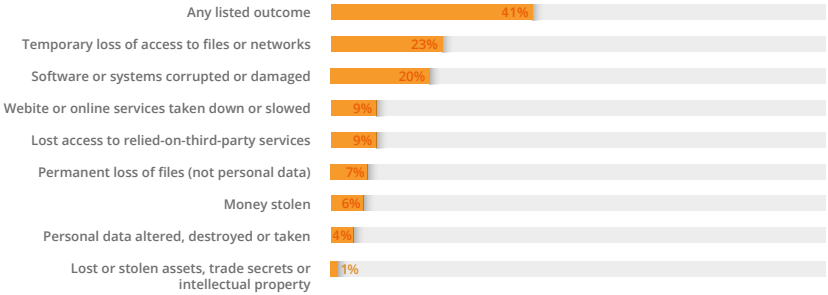
CYBER SECURITY BREACHES SURVEY 2017

TYPES OF BREACHES SUFFERED AMONG THOSE WHO HAVE IDENTIFIED BREACHES



Base: 781 that identified a breach or attack in the last 12 months

OUTCOME OF BREACHES AMONG THOSE WHO HAVE IDENTIFIED BREACHES IN THE LAST 12 MONTHS



Base: 781 that identified a breach or attack in the last 12 months

WHETHER BUSINESSES HAVE INCIDENT MANAGEMENT PROCESSES AND CONTINGENCY PLANS

Bases: 1,523 UK businesses (*761 that identified a breach or attack in the last 12 months); 506 micro firms (*179); 479 small firms (*241); 362 medium firms (*229); 175 large firms (*112)

The Risks From Cyber

Organisations in all sectors are at risk from cybercrime. Whereas traditionally assessing the cyber risk to an organisation may have been the preserve of government and large financial institutions, this is no longer the case. Charities are not immune to cyber criminals, and are increasingly under attack.

What is at risk?

As a charity, your money, your reputation, your data, your intellectual property and your IT equipment and systems are all at constant risk. This can be systems that interact with donors, such as websites and payment systems, but can also be internal systems and files

Who poses a threat?

There are a range of threat actors that may wish to target all or elements of your organisation, these include:

Malware

The term malware refers to malicious software. Software, that operates as malware, is designed to gain unauthorised access to devices or networks, and either disrupt their operation or gather information from them.

Infection from malware can come from a range of sources. These include:

1. **Contaminated email attachments**
2. **Infected websites, apps and adverts**
3. **Files stored on external devices such as mobile phones, computers and USB drives**

Types of Malware

SPYWARE

This type of malware is designed to steal information about your activity on a computer or other device. It is capable of a range of functions including screenshots, taking over cameras and microphones and recording key strokes. This enables criminals to gain information they can use, such as internet banking passwords.

RANSOMWARE

This is a form of malware specifically targeted with denying access to files and data. It is often very easy to be tricked into opening an email or file that contains ransomware, which can result in all of your files becoming unusable. Once the files become locked, the criminals contact the victim asking them to pay a fee (ransom), to regain access to the files or data. Payment is often by a hard to trace route, such as Bitcoin.

VIRUS/WORM

Both viruses and worms infect host systems and then spread to infect others. Once on a system they insert copies of themselves into programmes and files. They can also carry other things with them (payloads), designed to perform harmful activity on the systems they infect. This type of malware can cause rapid, widespread damage. For example, worms can enable attackers to create a group of hijacked machines called a botnet. This can then be used to carry out further attacks, such as distributed denial of service (DDoS) attacks.

Protecting Against Malware

Antivirus software should be installed on all computers, devices and servers. It will monitor, and often remove, malware when it's detected and will also often repair damage that may have been caused. It is imperative that antivirus software is kept up to date, this may be called 'updating' or 'patching'. Making sure that the latest version is installed will ensure that you are protected against the most newly developed malware variants.

USE A FIREWALL

A firewall is designed to provide protection between interconnecting networks of computers. It controls the traffic that enters and leaves a network and can be used to set up rules that allow or don't allow specific types of traffic to come through. The most common use of firewalls is to create a protective barrier between an organisation's network or trusted environment and the internet or untrusted environment.

BACK UP

It is important to ensure that backups of vital data happen regularly. There are many different ways to back-up data including cloud storage, external hard drives and tapes. However back-ups occur, they should be checked to ensure they are working and be encrypted to ensure they are safe and protected.

CONTROL DEVICES

Restricting what devices are able to connect with and connect to can prevent malware from entering and spreading between computers or networks. Stopping computers being able to have USB devices or connect to smart phones may reduce the chance of malware entering the computer, but it's always important to consider the user experience and how users will go about their work. As a principle, restrict all devices to be able to do the minimum needed to be able to carry out business. This is helpful in reducing the potential for devices to have impact when compromised with malware.

USERS - BEWARE!!

- BE CAREFUL FOLLOWING LINKS
- BE CAREFUL OPENING ATTACHMENTS
- DON'T CLICK ON ADVERTS
- IF IT'S STRANGE – REPORT IT

Social Engineering

Phishing

When fraudsters and criminals are trying to socially engineer, it means they are trying to trick people into assisting with their criminal activity. Cyber criminals are increasingly using a number of techniques to trick users into sharing information, unknowingly granting access to systems and networks, and sometime tricking people into sending money to those who shouldn't receive it.

A

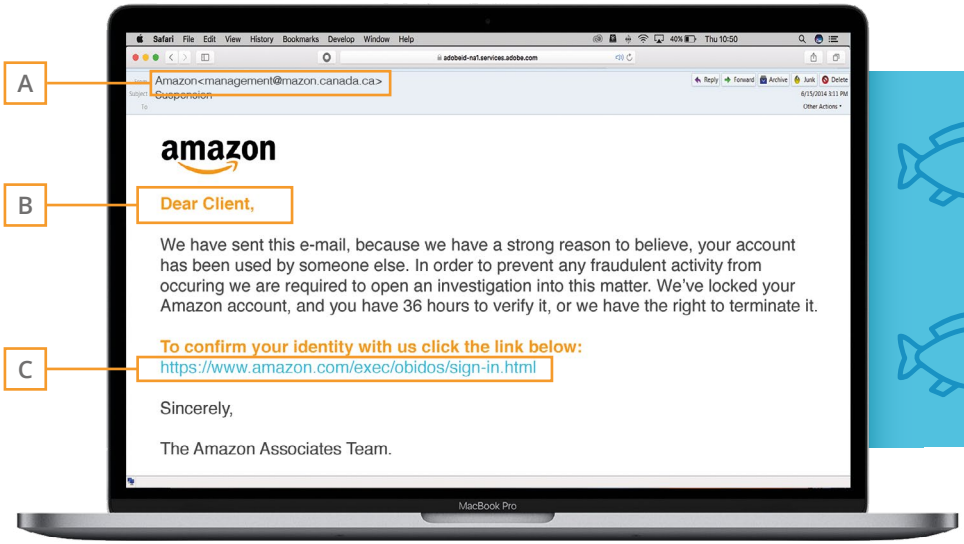
Not an Amazon email address (note the missing A in 'Amazon')

B

Generic non-personalised greeting

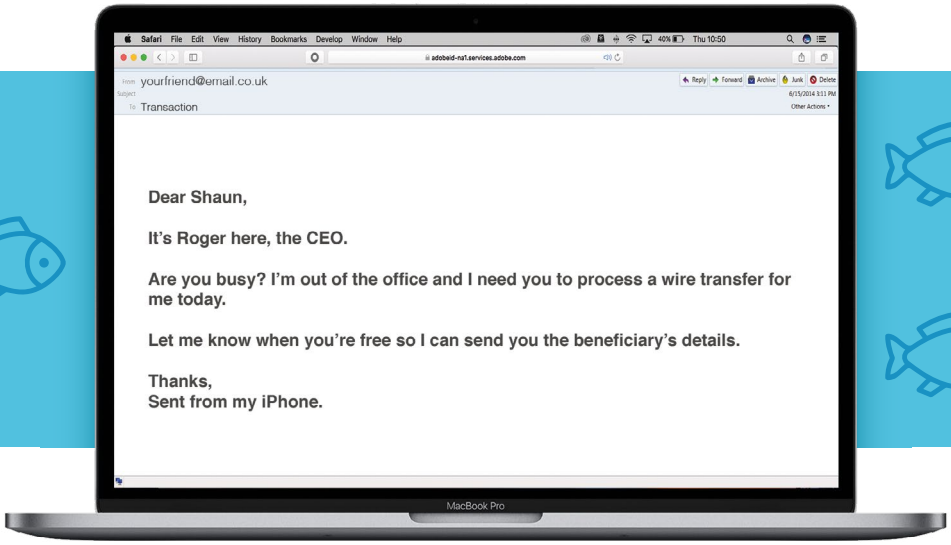
C

Hovering over the link reveals it points to a non-Amazon site "https://redirect-kereskedj.com"



Spear Phishing

Spear phishing is a more direct and targeted form of phishing. As with Phishing above, cyber criminals will send emails, however they will be specifically targeted at a person and the apparent 'sender' is likely to be someone the recipient knows.



Protecting Against Social Engineering Attacks

CHECK THE EMAIL ADDRESS

Check that the address isn't appearing as a different address. You can hover over the email address to see the real sender's address, although this can be disabled. Checking the header of the email will also show the true sender's address.

CHECK REQUESTS

It is rare for organisations to request personal information or login information via email. Should a request be made, don't reply to the email, find a known route to contact the organisation to check before sending; this could be an online portal or a phone number that is on a letter, their own website or an internet search.

VERIFY IF CHANGES ARE NEEDED OR PAYMENTS NEED TO OCCUR

As with personal details and login information, check with a specific person within the organisation requesting the payment before transferring any funds. This should also be done using established or trusted contact details, not by replying to the email you have received, even if it looks convincing.

Continuing to Protect Your Charity From Compromise

OUR ADVICE

- Always change default passwords
- Consider user secure password-saving technology
- Only ask users to re-set passwords when there is a suspicion of compromise (i.e. not every 6 weeks)
- Do not select passwords that are easy to guess, or that may be common
- Select passwords that combine a number of short random words or a phrase, as these are often easier to remember
- Set up accounts to lock when there have been multiple attempted failed logins.

Be Wi-Fi Aware

Wi-Fi that is publicly available can be a quick and useful solution when travelling or away from work or home. However, not all connections are secure and cyber criminals may be attempting to intercept your data.

Good Practice Cyber Protection

Have a Cyber Strategy and a Risk Management Scheme

IT Lab can support you in establishing the organisational risk of cyber, the current posture of your estate and the gaps or vulnerabilities you may have. Once established, IT Lab can help you to pro-actively plan, to continuously monitor and ensure your organisation has a robust approach to dealing with the risks that we all face in a fast evolving world. When assessing your risk management regime and associated mitigations, considering the following security areas can help to achieve adequate defences for your charity.

NETWORK SECURITY

Although not the entire answer to security and protection, it is important to defend the network perimeter, filter unauthorised access or attempted access, and malicious content. Continually monitor devices and test security controls.

USER EDUCATION

Ensuring all users are aware of cyber threats and how to prevent them can be a huge advantage in tackling cyber criminals. Produce user security policies covering use of systems. Train staff on how to act if they are suspicious and how to use systems and tools. Continually maintain awareness of the cyber risks your organisation faces.

MALWARE PREVENTION

As we have visited previously, take steps to prevent malware and include anti-malware defences. Continually ensure devices and software are up to date.

SECURE CONFIGURATION

Create an inventory of systems and devices. When managing devices define a baseline build for all types of devices and ensure it is followed and updated. Continually apply security patches and ensure configuration and updates are maintained.

MANAGING PRIVILEGES

When creating and administering users, limit user privileges to the minimum required set and monitor user activity. Control access to the activity and audit logs. Limit the number of privileged accounts and consider using tools for management of this type of access, in tandem with effective management processes.

INCIDENT MANAGEMENT AND RESPONSE

Establish management processes and ownership of incident identification, escalation and management. Implement an incident response and disaster recovery capability. Continually test incident management plans to ensure they remain effective.

MONITORING

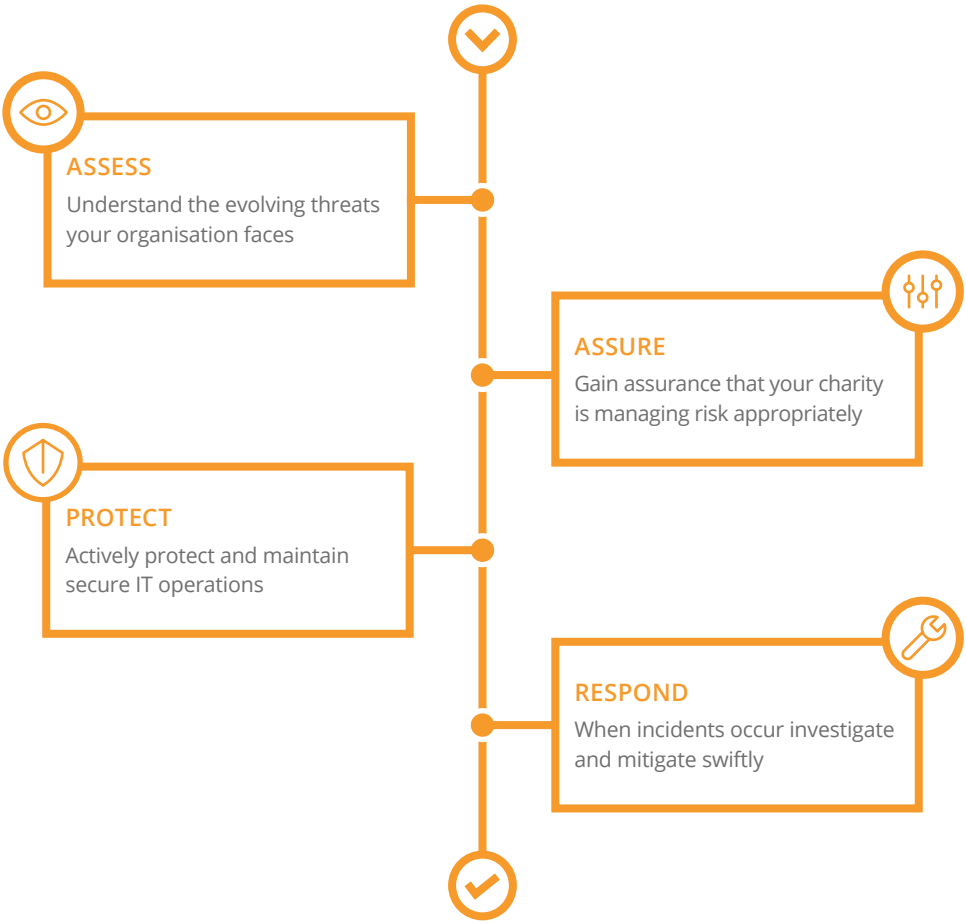
Establish a monitoring strategy and generate supporting policies and guidance. Implement a monitoring capability or capabilities. Continually monitor all systems and networks, and analyse logs and events for evidence of attack.

HOME AND MOBILE WORKING

As described in secure configuration, ensure the baseline build is applied to all devices and that the devices can be managed. Protect and encrypt data in transit and at rest. Train staff to adhere to the mobile working policy, whilst providing them with technology that appropriately mitigates the risks.

How IT Lab Can Help You Avoid Becoming a Victim of Cyber Crime

IT Lab provides the necessary capabilities to deliver flexible yet comprehensive cyber risk management for your charity.



Addressing Cybersecurity Risks

WHAT IS THE SITUATION?

Charities are increasingly exposed to the changing and pervasive landscape of cyber threats

WHAT ARE THE CHALLENGES BEING FACED?

- Lack of understanding and capability within charities to be able to assess risks and current posture
- Cybersecurity has often not had focus and it is assumed that it's being done (e.g. by IT provider/team)
- Increasing complexity in range of systems and devices, along with increased connectivity to other services and third parties
- Uncertainty where to start and what an appropriate level of cyber assessment and assurance is (both effort and cost)

WHAT ARE THE CYBER PRODUCTS?

- Cyber Risk Assessment/Due Diligence
- Managed Assurance Service
- Targeted Penetration Tests
- Monitoring and Security Operations Centre

WHAT WILL WE DO?

- Cyber Risk Assessment to give overview of likely risk
- Open Source Intelligence Assessment to give an overview of external footprint on the internet
- Phased technical assessment and testing to establish level of 'Cyber Hygiene' within the environment
- Phased Social Engineering testing to establish people centric risks
- Training of users to highlight risks and importance of security
- Penetration testing on specific high risk targets
- Security Operations Centre Service (SOC)

Elements of the Managed Assurance Service

OPEN SOURCE REPORTING

An Intelligence report specific to your organisation to assess what information is available and how hackers view this information. We also assess the risks that the data could expose you to and the ways in which it could be used to technically exploit your systems and your people.

SOCIAL ENGINEERING

Mock Phishing campaigns to target all staff. This includes the execution of phishing campaign(s) of varying sophistication to assess the level of risk posed by your people.

We also carry out a physical social engineering attack where we attempt to gain access to your office/buildings.

ONLINE USER TRAINING

We will set up a specific instance of our training platform for your people to use. This will enable continuous training using highly interactive content and quiz questions.

CYBER RISK DUE DILIGENCE ASSESSMENT

Assessment of the cyber risks faced by your charity through interrogation of the polices and procedures you currently have in place to provide a baseline for further development and improvement. This is carried out through interviewing and a review of current procedures.

HEALTH CHECK & CYBER ESSENTIALS

Quarterly assessment of a technical control area from Cyber Essentials PLUS. This covers boundaries, patching, configuration, access control and malware testing. This is carried out through technical assessment of elements of infrastructure. We will also carry out a formal CE+ assessment towards the end of the year.

VULNERABILITY SCANNING

Continued scanning of elements of your infrastructure will enable us to assess possible vulnerabilities that could be exploited over the internet. Specific elements of scanning or testing will also be carried during the Cyber Health Check and Cyber Essentials Certification process.

“Our approach is very collaborative. We like to educate, guide and upskill at the same time.”

Pravesh Kara - Head of Cyber Consultancy, IT Lab

GET IN TOUCH...

hello@itlab.com

0333 241 7689

www.itlab.com

“Our responsibility to our clients and supporters, in terms of their data privacy, is something we think about every day. For us, selecting a trusted security provider was paramount. IT Lab’s cybersecurity team has become an extension of our IT team. It’s not just about their technical capabilities, which are exemplary – it’s about their attitude. They are highly responsive and share their knowledge and insights.”

Laurence Crummay -
IT Project Management Team Leader,
Christians Against Poverty

“The output was very insightful, we were impressed at the things they could find both about our technology and how our people use the internet.”

IT Lab Client - Professional Services

London
2nd Floor
40 Bernard Street
Bloomsbury
London
WC1N 1LE

Manchester
Lowry Mill
Lees St
Swinton
Manchester
M27 6DB

www.itlab.com