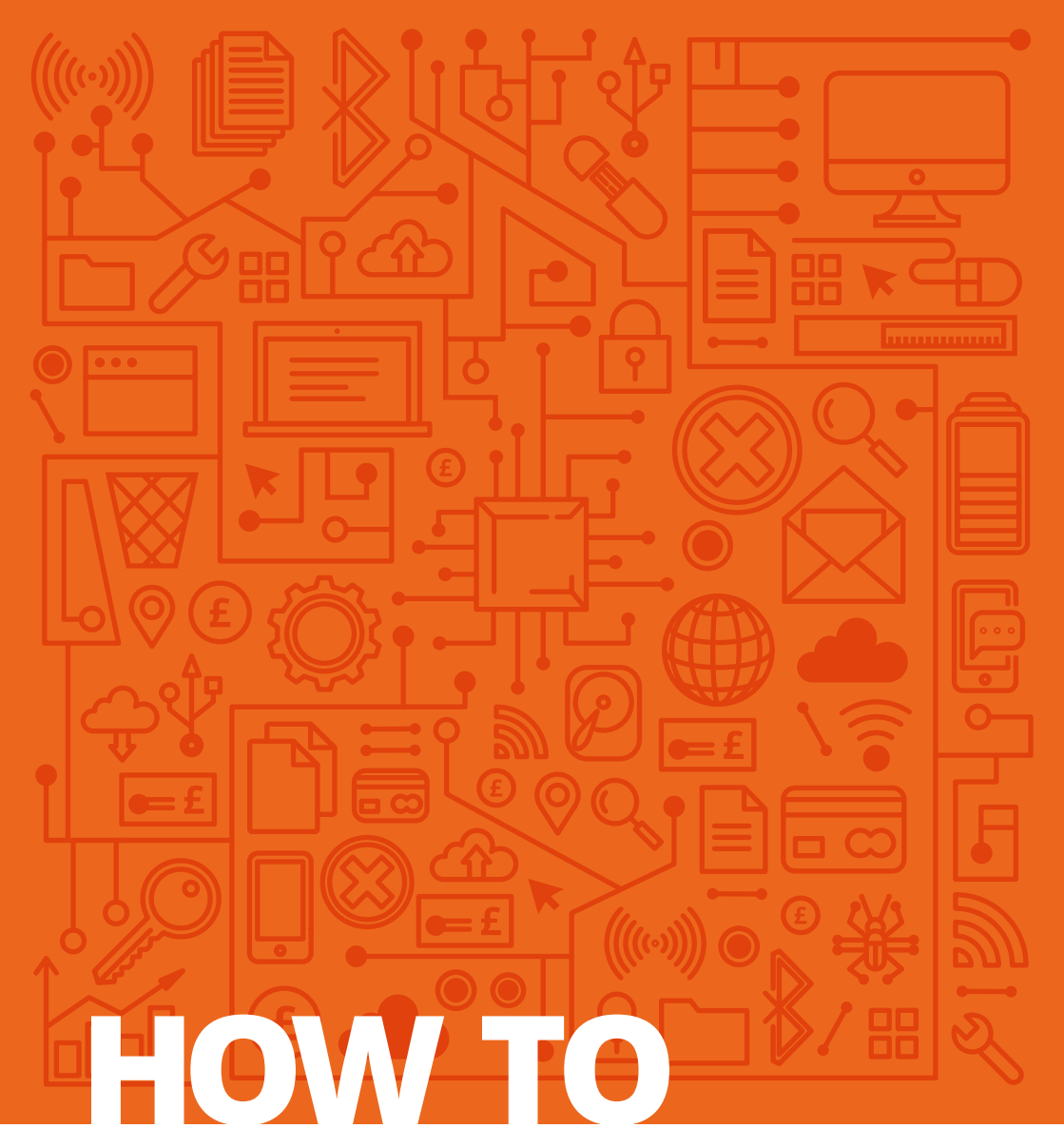


HOW TO

Protect Your Business In An Evolving Digital World

A non-techie guide to the risks, threats and mitigations for businesses.

itlab

We believe that data is the phenomenon of our time. It is the world's new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true – even inevitable – then cybercrime, by definition, is the greatest threat to every profession, every industry, every company in the world."

- Ginni Rometty, IBM's CEO

Table of Contents

03.
Current Cyber Trends

05.
Business Risks From Cyber

06.
Malware

07.
Protecting Against Malware

09.
Social Engineering

12.
Good Practice Cyber Protection

14.
How IT Lab Can Help You Avoid Becoming A Victim of Cyber Crime

15.
Addressing Cyber Security Risks

16.
Elements Of The Managed Assurance Service

Current Cyber Trends

All businesses rely on the internet; it is core to how most businesses engage with customers, partners, employees and suppliers. However, it's important to remain aware of the risks, as well as the opportunities, that are presented by this connectivity.

Computer systems in businesses of all sizes are attacked thousands of times a day across the globe. The nature of the threat we all face is significant, growing and increasingly diverse. This means that it's likely that some attacks will get through. At IT Lab - incorporating Perspective Risk, we help to manage and mitigate the impact of those attacks.

In 2017, we have seen the continued evolution of ransomware with WannaCry grabbing headlines after affecting a number of networks in the UK and parts of the NHS. NotPetya was able to cause significant financial losses across the globe affecting companies ranging from shipping and oil, to pharmaceuticals. Data breaches resulting from hacks and exploitation of vulnerabilities has also increased; 189M voter records exposed in the US, political campaigns hacked and 140M personal records exposed in the Equifax breach.

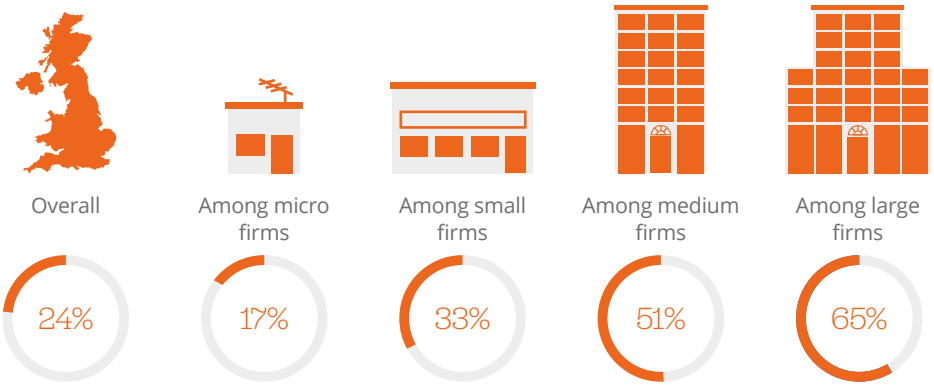
This increasingly complex landscape of attacks, data theft, influence operations and ransom demands has become normal in 2017 and will continue to evolve. In the UK 66% of medium and large UK businesses identified at least one breach or attack in the last year.

The most common types of breaches related to staff receiving fraudulent emails (72% of those who identified a breach or attack), followed by viruses and malware (33%), people impersonating the organisation online (27%) and ransomware (17%).

The UK is facing an exponentially increasing epidemic of cyber-crime. The increase in capability and diversity of threat actors, coupled with chronic underreporting, is enabling the criminal practices to thrive. At IT Lab, we are committed to protecting businesses from the evolving cyber threat; we hope this document provides useful insight and tips to help you to start to manage your personal and business cyber risk.

Michael Bateman
Director of Cyber Services

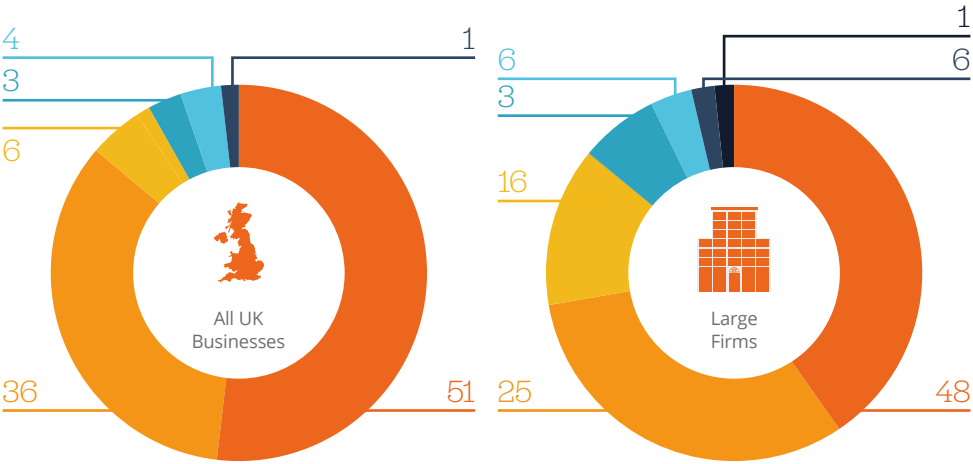
PROPORTION OF BUSINESSES THAT HAVE HAD BREACHES IN THE LAST 12 MONTHS?



% Experiencing a cyber security breach or attack in the last 12 months

APPROXIMATELY HOW OFTEN IN THE LAST 12 MONTHS DID YOU EXPERIENCE CYBER SECURITY BREACHES OR ATTACKS?

- % Only once
- % Less than once a month
- % Once a month
- % Once a day
- % Once a week
- % Several times a day
- % Don't know



Cyber Security Breaches Survey 2016, Department for Culture, Media & Sport

Business Risks From Cyber

Businesses in all sectors are at risk from cyber-crime. 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. Businesses that find themselves in the supply chain of larger organisations, legal firms and professional services firms, where businesses have access to other firms' data, processes and systems, are all increasingly coming under attack this list is however by no means exhaustive.

What is at risk?

As a business 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 customers, 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 business, 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 a business network or trusted environment and the internet or untrusted environment.

BACK UP

It is important to ensure that backups of corporate or important 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

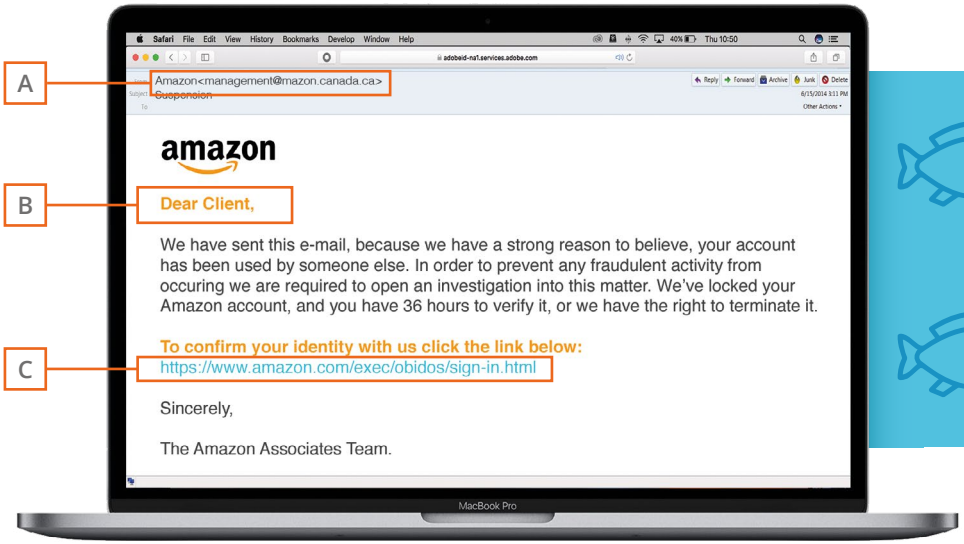
Not an Amazon email address (note the missing A in 'Amazon')

B

Generic non-personalised greeting

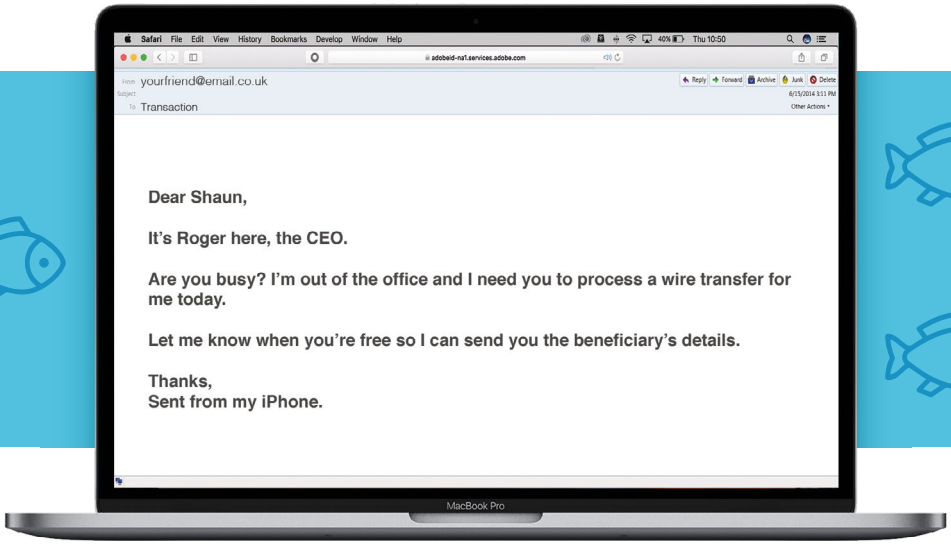
C

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



Spear-phishing

Spearphishing 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 organisation 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 & a risk management scheme

IT Lab can support you in establishing the business 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 organisation.

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

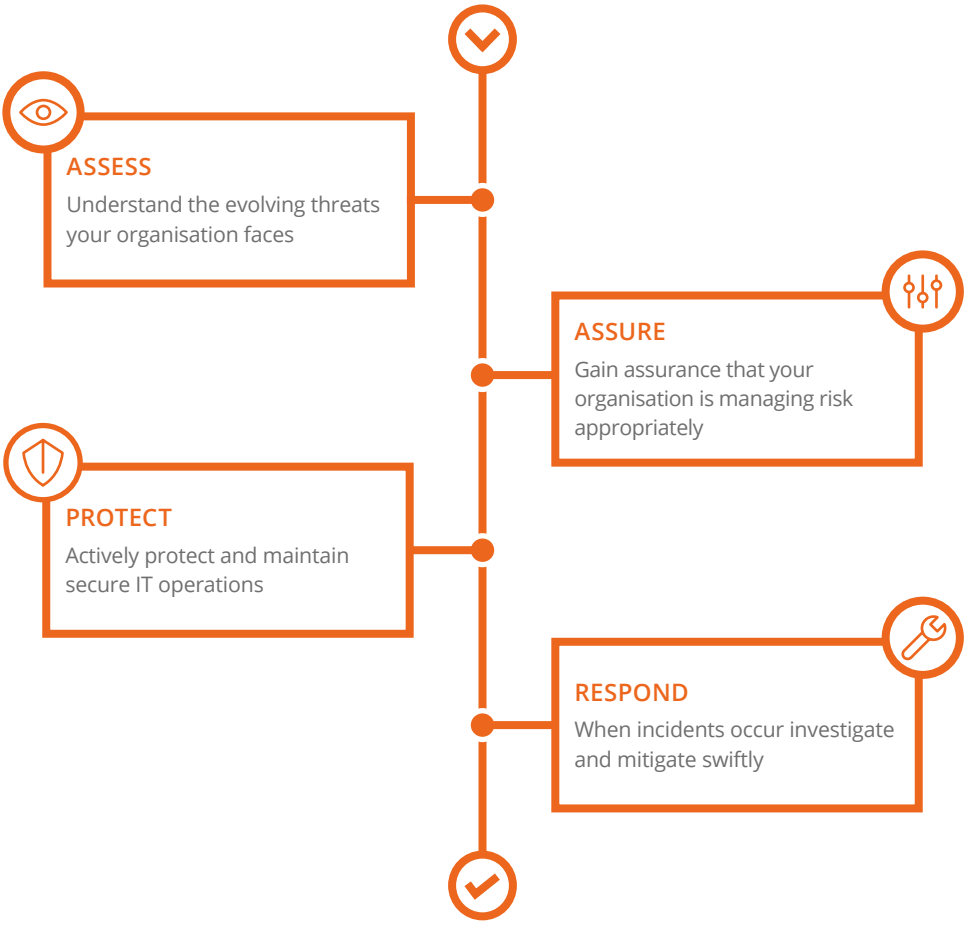
Establish a monitoring strategy and generate supporting policies and guidance. Implement a monitoring capability or capabilities. Continually monitor all systems and networks, and analyse logs and events for evidence of attack.

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 business.



Addressing Cyber Security Risks

WHAT IS THE SITUATION?

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

WHAT ARE THE CHALLENGES BEING FACED?

- Lack of understanding and capability within organisations to be able to assess risks and current posture
- Cyber security 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 organisation 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.

“

Even though we take security seriously, the additional operational capability that we now have through the IT Lab Cyber Team helps us to protect ourselves as fully as we now need to”

IT Lab Client - Financial Services

GET IN TOUCH...

 hello@itlab.com

 0333 241 7689

 www.itlab.com

“

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

“

We got to see gaps in many aspects of our security - our buildings, our people, our presence on the internet and the IT systems and apps we use”

IT Lab Client - Hospitality

itlab

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

Manchester
Lowry Mill
Lees St
Swinton
Manchester
M27 6DB

www.itlab.com