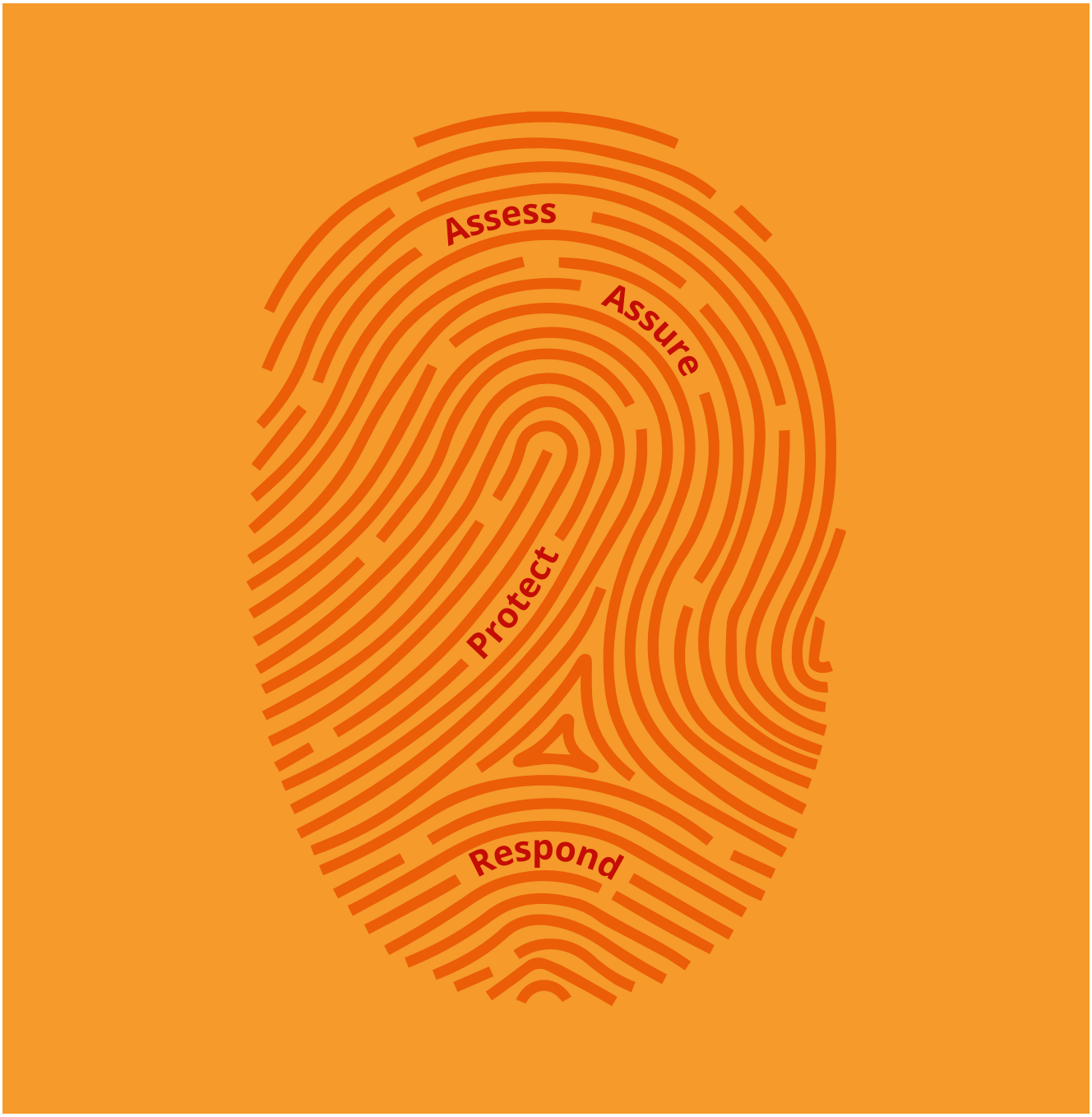
Greater Manchester Chamber of Commerce
Chamber of the Year 2017/18



Chamber Secure

Comprehensive Cyber Risk Management Services

Powered by IT Lab

Introduction

"The UK is facing an exponentially increasing epidemic of cyber-crime."

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 the UK 66% of medium and large UK businesses identified at least one breach or attack in the last year.

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. This is why we have partnered with the Greater Manchester Chamber of Commerce to give Chamber members access to comprehensive cyber risk management services.

Michael Bateman - Director of Cyber Services at IT Lab

Assess:
Open Source Intelligence

How much information are you providing about your organisation on the Internet?

You may answer "a lot", you want your business to be easily found right? Unfortunately, in doing so, you are also most likely putting information out there that can be used to cause your organisation harm.

Threat actors thrive on this inadvertent leak of information as it not only allows them to focus their plans on compromising you but also allows them to come across more credibly to you and your staff. Credibility builds trust, which is then manipulated by a threat to make a gain, and for you to suffer a loss as a result.

So what kind of information is useful to a threat?

They are predominantly looking for contact details of people who work in your organisation, their email address, their job role. Cyber criminals love to focus on executives and finance roles so that they can manipulate the actual movement of money, such as asking for a transfer or modifying bank account details on invoices.

They are also looking to understand what technology you use. In understanding the make, model and versions, they could potentially unearth a vulnerability that they can exploit to breach the security of your applications and systems.

Other useful information involves understanding if any of your users have been breached in the past so they can obtain the passwords and try them on your systems.

What can IT Lab do to help?

Our cyber experts can undertake a discovery exercise to establish just how big an exposure you have that can be leveraged by a cyber criminal. Our approach taps in to the same repositories and uses the same tactics that threat actors use in profiling you. The only difference being that we'll put this in a report and put some context around it so that you can act on the results and reduce your exposure.

Summary:

Assess: Open Source Intelligence	> Identify your sensitive information in the public domain
	> Receive a report on your exposures that criminals can exploit
	> £450 ex VAT. (Includes 25% discount for members)

Assess:
Common Attack Simulation

Business Email Compromise: The most successful criminal money making attack

There are many cases of organisations and individuals getting "hacked" in the media. However, these are the ones that have had to be disclosed or the victim has chosen to disclose to show they are doing the right thing. These are also only the tip of the iceberg. Individuals as well as organisations have been falling foul to what look like sophisticated targeted attacks through email, however, these largely go unreported. The losses are dealt with internally and are not even reported to the authority for fear of significant negative damage of hard built reputations. Having been involved first-hand in many cyber investigations in the last year, IT Lab can substantiate the significant financial losses incurred by organisations and by individuals.

Why is it so prolifically successful?

Put simply, human psychology and a lack of awareness. This type of attack starts off with a human vulnerability that then escalates to a business process vulnerability via manipulation of your technology. An email usually comes in to a user in your organisation, normally with a link to a document, or sometimes with a document attached which contains a link. The email message is not usually targeted, but is convincing enough to motivate a user to click the link. The link takes them to a page (on an already compromised website) that looks like the login page for well known email software, Office365, G-Suite, etc. Unfortunately unsuspecting users sometimes enter their real usernames and passwords in to these fake websites. That is when the trouble starts. As soon as a cyber criminal has those credentials, within a matter of hours they will have logged on to the user's email account, rifled through all the sensitive emails, concocted a plan to manipulate a business process, such as modifying and resending invoices, and made changes to prevent their detection. The result? Often, a large sum of money is transferred to a criminal controlled bank account, leaving the organisation or individual to pick up the pieces, often wondering why they were targeted. Once the account has been "burned" by a criminal, they will use it as a platform to spam the user's contacts to jump to their next victim.

What can IT Lab do to help?

We assess how susceptible your organisation is by simulating the same behaviour as these cyber criminals, without stealing your money of course. We start with just your company name, expand that knowledge to who works for you, then send phishing emails to the individuals. We then monitor for user activity throughout the simulation and report back to you to rationalise the scale of the problem.

Summary:	
Common Attack Simulation	> Simulate the most prolific and most successful attack method used by criminals – phishing > Starting with just your company name, we'll identify your users and attempt to phish them > £1,800 ex VAT. (Includes 25% discount for members)

Assess:
Technical Vulnerability Assessment

The scale of the problem

Technical vulnerabilities are problems with software that allow the software to be used in a manner that was not intended by the author. These are often exploited by cyber threats to break in to systems and applications, with the aim of stealing data or using your resources, amongst many other nefarious motivations. There are thousands of vulnerabilities that have been reported publicly, and many more that haven't. To give you an idea, in 2017 alone, there were 18,114 vulnerabilities registered in one of the main vulnerability databases on the Internet. That equates to an average of 49 new vulnerabilities becoming known every single day in 2017.

How often do you check for vulnerabilities?

All it takes is one vulnerability to gain a foothold on to your systems, application or network. Are you checking for vulnerabilities more often than the criminals are? Cyber threats will usually undertake sweeps of the Internet looking for specific vulnerabilities, often the latest ones, as they take advantage of people being slow to patch their systems even when they know there is a patch available. If you were monitoring your systems, you would likely see sweeps for a new vulnerability within hours if not minutes of a new vulnerability being published, that is how quickly threats react to this information.

What can IT Lab do to help?

The most conclusive way to understand your vulnerabilities and whether they actually present a material risk to you is through a process called a "penetration test". These are undertaken by highly skilled and experienced ethical hackers who replicate the behaviours of real cyber criminals to identify and exploit vulnerabilities. However, for most organisations, running a penetration test more than once a year is usually cost prohibitive.

A more sensible way of regularly identifying potential vulnerabilities is through conducting a Technical Vulnerability Assessment. This uses well documented vulnerability signatures to discover vulnerabilities on your perimeter, i.e. the element of your systems and networks you expose to the Internet. Vulnerability scans are conducted with tools and can be automated to a certain degree so are more cost-efficient when wanting to understand your vulnerabilities more frequently.

Summary:

Technical Vulnerability Assessment	> Undertake a technical vulnerability scan of your perimeter to understand your exposure. > £200 ex VAT for a one off scan. Or, Quarterly scanning for £600 ex VAT (Annual contract)

"In the UK 66% of medium & large UK businesses identified at least one breach or attack in the last year."

Assure:
Cyber Health Check

The State of UK Businesses

The UK Government's security arm, NCSC (National Cyber Security Centre) has been monitoring cyber security breaches for many years and has been analysing what the root causes are and whether there are any trends. It turns out there are, and they found that most breaches could easily have been avoided by applying simple defences at little to no cost. NCSC, together with established professional cyber security standards organisations, used these trends to create an assurance scheme called Cyber Essentials. Additionally, they provided a means to certify against the scheme so that organisations that undertook the challenge could recognise and be recognised as an organisation that takes its cyber security seriously.

The UK Government as a whole now recognise the value in this certification and require suppliers to be certified to this scheme or working towards this scheme if you want to bid for a government contract. Other private organisations are also adopting the same approach in their supplier selection as a minimum cyber security standard.

What can IT Lab do to help?

Our Security Consultants can review how you measure up against the Cyber Essentials scheme and identify any gaps. The review is a deep dive in to your policies, processes and technical security measures which results in a robust assessment against the scheme. The gaps are analysed and documented in a report together with recommended steps on how you can remove the gap and meet or exceed the baseline set by the scheme. Undertaking this review will give you confidence and get you closer to certification than any other method.

When you think you are ready, we can also help certify you through our certification body, Perspective Risk. Perspective Risk, whilst owned by IT Lab, is a separate legal entity with its own certifications, processes and people to maintain independence from its parent.

Summary:

Cyber Health Check	> Gain assurances on the most basic defenses needed to survive in the UK as advised by the UK Government's Cyber Essentials standard > We dive in to your basic controls to understand strengths and weaknesses and provide remediation guidance > £2,000 ex VAT. (Includes a 25% discount for members)

Protect: Security Awareness

Why is awareness needed?

Technology has advanced rapidly over a very short space of time. Whilst the benefits are immense, often, technology products and services are brought to market with the assumption that the user is in some way "technical". In reality, most users are not technical, technology is a means to an end, to support a workflow, or a business process, and ultimately the business. What we've ended up with is a gap in assumed knowledge of technology, which also infers users know how to use technology securely.

In the meantime, users will be blamed and called the weakest link when an organisation is breached. Incorrectly, we might add. Whilst the gap is getting smaller and technology is addressing this poor assumption, it will not arrive in a short timeframe. IT Lab's Secure By Design concept is also not quite a reality for most technology based solutions. It is for this reason that awareness is needed to bridge the gap and highlight the risks to information and information systems in your organisation.

What can IT Lab do to help?

IT Lab has developed an online portal that delivers training at the user's pace in short but engaging awareness modules. Each module covers a key facet in cyber security including how to handle corporate information, email security, internet security, social media security, phone security, and physical security. The content includes a short bite-sized video, all less than 10 minutes in length. This is then followed up with a short quiz to verify comprehension and retention.

The designated administrator can then regularly download reports to monitor progress for the organisation to ensure training is being undertaken by all staff.

Summary:

Security Awareness Training	> Increase your company's ability to spot cyber-criminal activity
	> Engaging online training portal access for 1 year including quizzes for maximising knowledge retention and comprehension
	> £1 per user per month ex VAT. (Annual contract)

Respond: Breach Response

Suffered a breach?

Once a breach has been identified, the first steps should be to contain the incident to ensure it does not spread. For this you need a well-rehearsed incident response plan. In reality, it is likely that organisations will not have an incident response plan, let alone a well-rehearsed one.

Containment requires quick response times to identify the source and limit its activity. This often requires specialist investigative and forensic skills. If you do not have this capability in house, the next best option is to have a 3rd party that can be called upon to react and undertake this activity for you.

Following containment of the incident, the next steps would be to eradicate all instances of malicious activity before restoring services and data where they were damaged.

When the incident has passed, undertaking a root cause analysis and incorporating lessons learned in to business processes and procedures is a vital step.

What can IT Lab do to help?

Initially, we can help guide you over the phone to contain the incident. IT Lab operate a 24x7 Secure Operations Centre manned by specialist security analysts and incident responders.

If you have suffered a cyber security breach then reach out to Lucy Mulligan on the Chamber's membership team by emailing benefits@gmchamber.co.uk or calling **0161 3934321**.

We can pass you to one of our experts who provide preferential rates for members.

Get in Touch

To discuss how these services can help you to mitigate the risks of the growing threats posed by cybercrime, please contact Lucy Mulligan at benefits@gmchamber.co.uk or calling **0161 3934321**.

IT Lab Client
Hospitality

"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
Professional Services

"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."

itlab

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

Manchester
Lowry Mill
Lees St
Swinton
Manchester
M27 6DB

www.itlab.com