# CYBER SECURITY FOR SMALL AND MEDIUM BUSINESSES

POOL RE
REINSURING TERRORISM RISK

MWR INFOSECURITY

# CONTENTS



## ABOUT POOL RE

Pool Re is the reinsurance scheme that underpins most of the terrorism insurance cover provided by commercial property insurers in Great Britain. Pool Re is an industry mutual owned by the UK insurance industry and was established in 1993 as a response to the market failure that was triggered by the IRA attack on the Baltic Exchange in the City. The costs of the IRA mainland bombing campaign in the 1990's led to reinsurers withdrawing cover for terrorism related damage, with insurers compelled to follow suit. Pool Re was founded by the insurance industry in cooperation with, and backed by a guarantee from Her Majesty's Treasury, to ensure that affordable terrorism cover could be provided to all who wished to purchase it.

Since its foundation, Pool Re has provided effective protection for the UK economy and currently underwrites in excess of £2.1 trillion of commercial property against damage caused by an act of terrorism. To date Pool Re has paid out claims of more than £600 million at no cost to the UK taxpayer. The scope of cover provided by Pool Re is very wide, including damage caused by chemical, biological, radiological and nuclear materials, but in 2018 cover was extended to recognise the possibility that in the future damage could be caused by remote digital means or cyber-terrorism. This extension of cover was the culmination of 3 years work to evaluate and quantify this new loss vector, and involved extensive academic research by the Cambridge Centre for Risk Studies.

POOL RE
REINSURING TERRORISM RISK

## ABOUT MWR

MWR provide specialist advice and solutions in all areas of security, from professional and managed services, through to developing commercial and open source security tools. We focus on working with clients to develop and deliver security programs, tailored to meet the needs of each individual organisation.

In a rapidly changing technology landscape, innovation is essential and our ambition to push boundaries sets us apart. Evidence of this approach is well documented on our dedicated research and development platform, MWR Labs. Our expertise in cyber security and incident response has led to MWR being a regular contributor to the annual Verizon Data Breach Investigations Report (DBIR). Central to MWR's philosophy is the desire to deliver high quality cyber security consulting services and unsurpassed levels of support to our clients.

MWR INFOSECURITY

# WHY YOU NEED TO MITIGATE CYBER RISKS

All businesses, from single person operations to large multinationals, increasingly rely on technology in various forms. Technology will likely underpin key revenue generation sources (such as production or retail) and much of an organisation's day-to-day running will be totally dependent on computer systems. As businesses and their assets become ever more tech-driven, criminals and other attackers are adapting and cyber attacks are increasing in volume and effectiveness.

A breach's impact varies depending on the attacker's goals. The attacker may be trying to commit fraud or steal money. Some seek intellectual property, others to cripple the organisation and charge a ransom to return the systems to working order. Many breaches carry indirect costs such as fines (up to 4% of global turnover under GDPR) and the reputational impact of a breach can be devastating.

Whilst organisations may assume that the technology they use (whether internally hosted or cloud) is secure, the reality is that attackers will exploit any weaknesses they find in configuration or usage. Managing this risk is difficult and many businesses lack board members with the necessary mix of technical understanding and authority to lead and challenge the organisation appropriately on cyber risks. Even organisations that do see cybersecurity as a strategic risk can find it hard to recruit suitably experienced security practitioners.

Despite the challenges, understanding and managing cyber risks is crucial for businesses of all size. It is also important that the effort invested in cyber security is proportionate to the assets the business has and the threats those assets face. This guide aims to be a first step for organisations wanting to manage their cyber security risks and provides threat centric advice for businesses of all sizes.

# BUSINESSES OF ALL SIZES NEED CYBER SECURITY

Cyber security is not the concern of governments and large businesses alone. A 2017 study showed that over 61% of data breaches took place in companies with fewer than 100 employees.

These events can have a rapid and lasting effect, especially for smaller businesses that may not have the capacity to survive significant business interruption. The impact of cyber attack can take a number of forms – intellectual property on which an innovative small business depends can be stolen. Critical data might be encrypted or destroyed. Administrative IT systems could be made useless. Businesses could be the victims of fraud. Or they may have sensitive personal data relating to customers stolen and misused. Destruction of data, theft of customer information, and financial compromise can cause significant loss of profit and reputation.

However, there are some simple steps you can take to ensure your business can withstand an attempted attack, and recover from it quickly should one get through. In fact, the Australian Government has assessed that over 85% of the attacks they investigated could have been prevented if just four technical controls were in place.

## CASE STUDY

A medium-sized organization in the energy sector was hit with a highly targeted ransomware attack. The attack used compromised admin accounts to push ransomware to multiple hosts, encrypting about 70% of the organization's data. Attackers then asked for a ransom of over $1 million. At the same time, attackers used more subtle malware to steal highly confidential information, assuming that it would not be noticed in the panic following the ransomware attack.

**Pool RE has partnered with MWR InfoSecurity to offer simple steps on securing your business.**

To get a sense of what guidance best suits your company, use the chart below as reference:

## SMALL BUSINESSES

You have a small, productive company of fewer than 100 people. You know security is important, but with so many hats to wear and so few staff, you need quick and easy wins to guard against cyber compromise.
Page 4

## MEDIUM BUSINESSES

Your company employs up to 1000 people and has a small IT team. You'd like to develop a more formal security program so the business can be as secure as it needs to be, but you need to ensure spending is in line with risk.
Page 5

## BEYOND

You've covered the basics and – if you haven't already – you're in the process of establishing a formal security role or small team. What comes next in building this team and planning the projects they'll support? Page 6

## WHALING: SOME OF THE MOST EXPENSIVE ATTACKS AREN'T TECHNICAL

Businesses of all sizes are increasingly targeted by a type of scam email known as "whaling" or "CEO fraud", with sometimes over £100m taken.

In whaling, messages are sent to financial staff and imitate an important team member (CEO, CFO).

**They typically contain the following:**

- Request for funds: "Invoice", "Wire to", "Tax requirement"
- Urgency: "Urgent", "Right now", "ASAP", "By end of business"
- Unable to confirm in person: "In meeting, can't talk", "Not at desk"

These attacks do not target computers and are hard to prevent through technical controls, instead requiring strong user awareness and business process controls to counter them.

### FOR MORE INFORMATION VISIT:

https://www.ncsc.gov.uk/guidance/whaling-how-it-works-and-what-your-organisation-can-do-about-it

## CASE STUDY

A small financial services consultancy had laptops that they ran themselves and used a cloud solution for emails and files. They had not configured two-factor authentication and did not discuss phishing risks.

A phishing attack led to a consultant revealing his sign-in credentials, which the attackers used to steal documents and attack the consultant's contacts by sending emails using his account.

**NEXT STEPS:** NCSC, Cyber Essentials Certificate helps organisations assess if they're covering the essentials: https://www.cyberessentials.ncsc.gov.uk/

NCSC, Small Business guide:https://www.ncsc.gov.uk/smallbusiness

# STEPS FOR SMALL BUSINESSES

**The Challenge: Limited dedicated resource**
Starting a security program in a small company can be difficult. Many organisations may not have a person focusing on IT full time (or will have 1-2 staff at most). Those enterprises will only have a very limited amount of resource to focus on security. However, even though the company size is small, the business will still face a variety of threats.

**The Approach: Security is everyone's job**
When resources are limited, it's more important than ever that security is part of everyone's job. Appoint a security champion to educate the team. This champion can improve their knowledge of security through basic training or certification, promote the security agenda, and advise on easy improvements to help keep the business safe. Promoting a culture where people take ownership for security is important. Even just having a way of sharing stories or concerns can help.

Equally key is minimising the security effort needed. Having modern operating systems that auto update and are more secure by default is important, as is considering cloud services that handle the security for you, to help reduce the effort needed.
The UK's National Cyber Security Centre recently issued some excellent guidance for small businesses. We cover some of the key actions on the next page.

## KEY ACTIONS

- Take regular backups of your important data and test that they can be restored.
- Protect against damage caused by malware, including by making sure that software is in support and kept up to date, using antivirus software (eg Windows Defender if you have a basic windows platform), controlling access to removable media, and switching on your firewall.
- Promote phishing awareness to prevent users falling victim to seemingly harmless emails that contain malicious content. Consider email protection solutions. Scan for malware and change passwords quickly if you suspect a successful attack has occurred.
- Keep employee smartphones and tablets safe, including by switching on PINs or password protection, and making sure all devices auto update. Make sure you don't install apps with wide ranging permissions **(see https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes)**
- Use passwords to protect your data. Employees should not reuse passwords between work and home. Use two factor authentication to access the most sensitive services. Look at using password managers.

# STEPS FOR MEDIUM SIZED BUSINESSES

**The Challenge: Limited time, lots of compliance**
Medium-sized businesses are likely to have a full-time IT team. However, resource for security is often still limited and may end up being focused on recovering from incidents or compliance with client requirements.

For a medium-sized business the “attack surface” – the range of services and assets that an attacker can target – is often larger than it would be for a smaller organisation. Medium-sized businesses are likely, for example, to be running company services and web applications that may have been deployed on a company intranet or the public internet. While many of these services are essential to support business growth, they will offer more opportunities for an attacker.

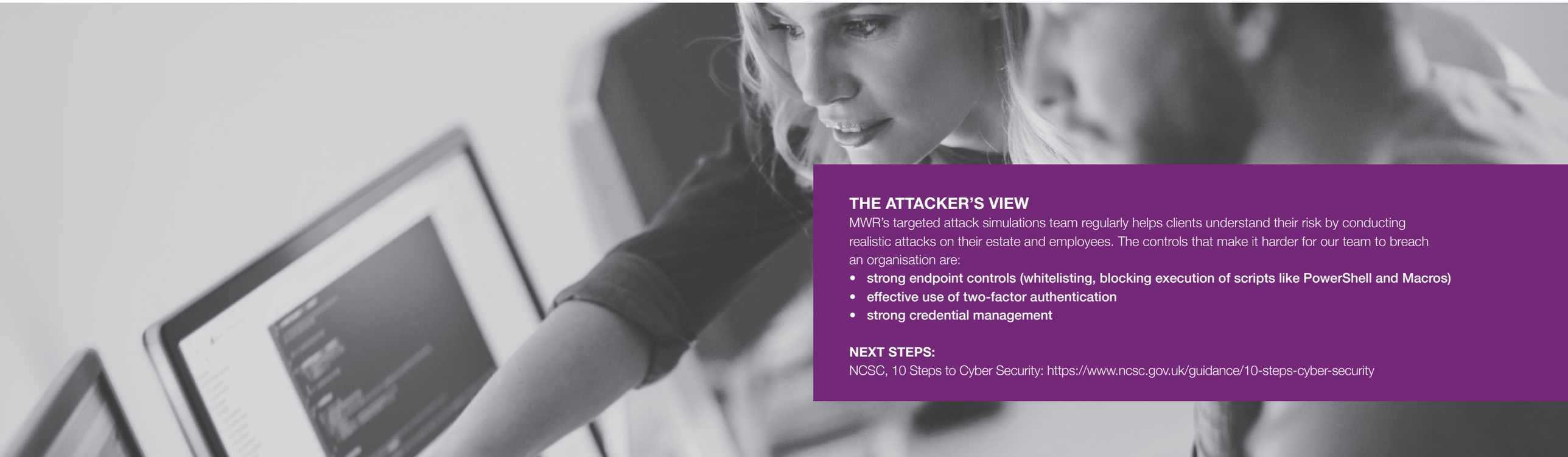
Moreover, the attractiveness of an organisation as a target is likely to increase with the company’s size and reach (particularly if it services clients in key sectors, such as defence or financial services).

**The Approach: Bring it to the board**
In a medium sized organisation, IT should have specific security responsibilities and reporting requirements.

The security team must work proactively with the business around it. If a security team has not been formed, appointing one or two individuals in IT to conduct a health-check and drive initiatives will ensure that high-priority issues get the right attention. Security and cyber risk should be a board level issue.

## KEY ACTIONS

- Understand your system, both hardware and software, ensure it is in support and all security updates are applied. Apply sound configuration policies to your IT estate. Take a look at the NCSC end-user device guidance and CIS benchmarks.
- Think about what services you expose to the internet and how you manage them. Use firewalls to protect systems available over the internet. Consider using an internet gateway. Implement network segmentation.
- Make sure users do not use high privileged accounts for standard functions like email and web browsing.
- Configure centralised storage of logs and conduct reviews looking for suspicious activity.
- Keep management informed of risk and risk reduction by explaining how each security measure helps to project the business’ interests. Make it a board issue.



## THE ATTACKER’S VIEW

MWR’s targeted attack simulations team regularly helps clients understand their risk by conducting realistic attacks on their estate and employees. The controls that make it harder for our team to breach an organisation are:

- **strong endpoint controls (whitelisting, blocking execution of scripts like PowerShell and Macros)**
- **effective use of two-factor authentication**
- **strong credential management**

**NEXT STEPS:**
NCSC, 10 Steps to Cyber Security: https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

# STEPS FOR GOING TO THE NEXT LEVEL

**The Challenge: Security as mature as your business**
As security becomes a more mature component of a business, a small team tends to support ongoing security developments. Often, management has agreed security is a priority, but isn't sure how to make sure security serves the business in the right ways.

The challenge becomes more complex as employees and premises expand. Clients are increasingly asking for evidence of security efforts. More services and applications are supported within the business, driving the need for a team to investigate and advise the business on the security of new solutions and increasing the number of potential attack paths.

**The Approach: Something more formal**
Security needs to become more formalised and bring together technical aspects with personnel and physical security.

Once basic security procedures have been implemented, projects of highest impact can be identified via formal reviews and risk management processes. These projects improve existing controls, provide awareness of new threats, and allow secure adoption of new technology in the business.

## KEY ACTIONS

- Establish robust governance processes are in place to enable you to understand and manage the risks.
- Create a risk management framework to support this work. Look at https://www.ncsc.gov.uk/guidance/risk-management-collection
- Ensure that personnel and physical security risks are understood and addressed, alongside technology risk.
- Develop a coherent programme of work to implement security improvements and monitor progress. Make this a whole organization response, not just something for IT.
- Make sure you are collecting all your logs, bring in some quality analysts to work on them, using a threat hunting approach. Identify and acquire the tools that would best support their work.
- Consider bringing in external experts to conduct an independent review of your security approach.
- Check your insurance coverage.

**NEXT STEPS:** CPNI, Security Passport: https://www.cpni.gov.uk/managing-my-asset/leadership-in-security/board-security-passport

# NEXT STEPS

Simple tools, built-in security features and new guides for small businesses mean staying secure is no longer the domain of large businesses alone.

With these tools, every minute invested in securing the business can help prevent a potentially significant loss of data, money and reputation.

## ADDITIONAL RESOURCES

**Phishing**
*Educate and train users on malicious emails*
- NCSC, Phishing: https://www.ncsc.gov.uk/phishing
- MWR, The Rising Tide: https://www.mwrinfosecurity.com/our-thinking/the-rising-tide/

**System Configuration**
*Create resilient systems*
- NCSC, End User Device Configuration: https://www.ncsc.gov.uk/guidance/end-user-device-security
- https://www.cisecurity.org/cis-benchmarks/
- MWR, Mobile Device Security: https://www.mwrinfosecurity.com/our-thinking/mobile-device-security/

*Security Controls*
- Top 20 Critical Security Controls: https://www.cisecurity.org/controls/

## DENIAL OF SERVICE: A LOW CAPABILITY ATTACK WITH A HIGH IMPACT

Attackers will sometimes flood a service with requests, either by abusing poorly configured public internet services or through hiring a botnet. Whilst the attack is ongoing, legitimate users are unable to access the targeted service. This can have huge cost implications, such as a payment service being unavailable during a busy retail period. For a case study see: https://statsdemo.mwrinfosecurity.com/studies/MWR_Threat_Intelligence_Case%20Study_DOS.pdf

Such attacks can often be a response to an individual becoming annoyed with an organisation and cannot be prevented. Instead, organisations are advised to ensure that critical websites are appropriately load balanced and able to tolerate spikes in traffic, potentially through use of third-party services.

Organisations should also ensure that critical servers that don't need to be internet connected aren't, so that an attacker can't impact critical, non-customer facing services.