outbound™ VIRTUAL

Cyber Resilience Guide

Table of Contents

outbound™ VIRTUAL

Section 1

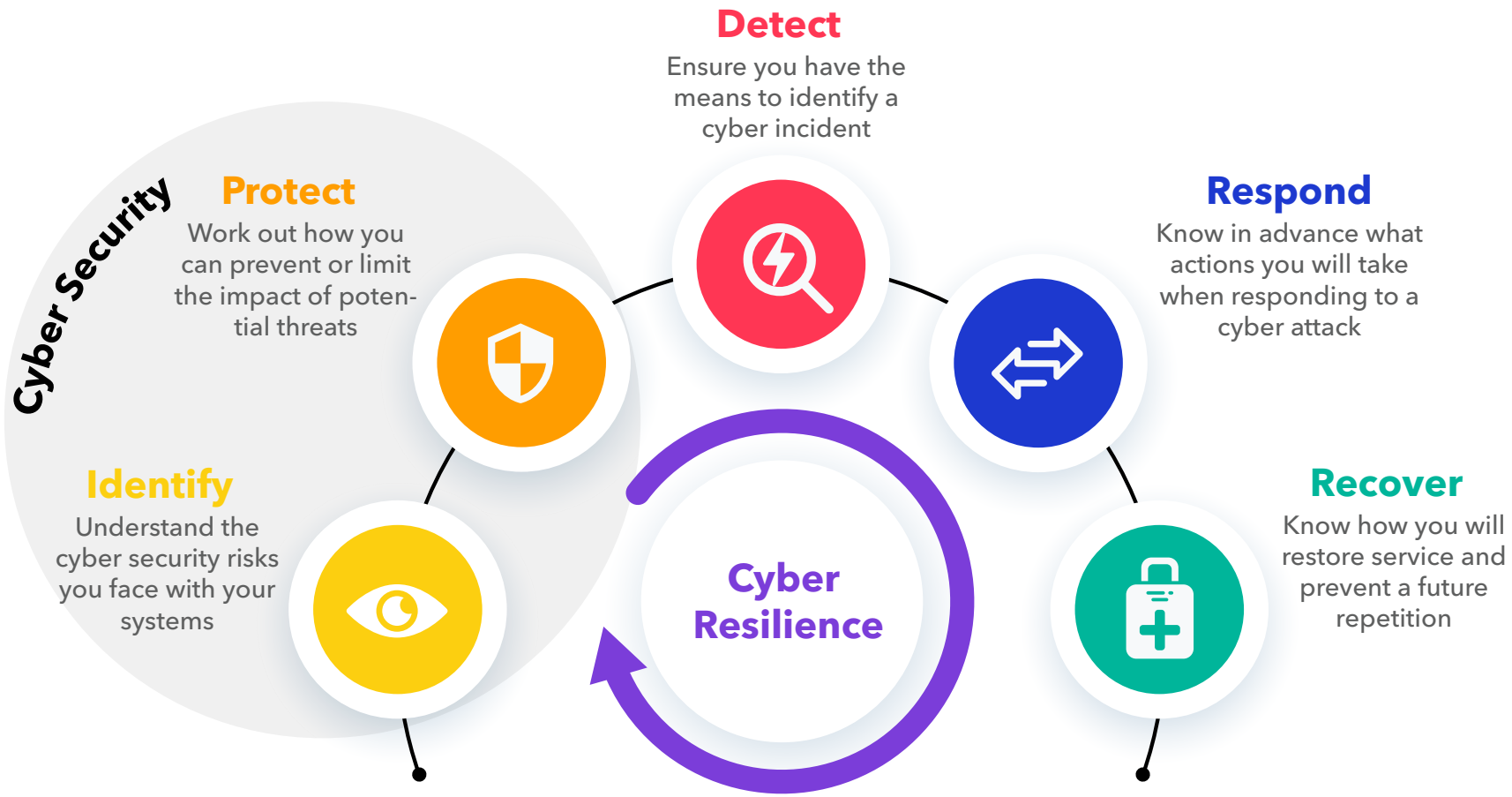
Introduction to Cyber Resilience

Despite the amount organisations spend on cyber security growing by 12% annually[1], on average someone falls victim to a cyber-crime every 39 seconds.

Cyber security is an organisation's ability to prevent and protect themselves from cyber-attacks. However, according to the UK government's 2023 Cyber Security Breaches survey 26% of medium businesses (50-249 employees) have fallen victim to a cyber-attack in the last 12 months[2].

So, what happens when the defences fail and how can we plan for the unknowns and worst-case scenario? This is where cyber resilience comes in.

Cyber resilience extends cyber security to include an organisation's ability to not only protect themselves from a cyber-attack, but to detect and recover from such an incident. The underlying principle is to accept that a cyber incident will occur, and putting the measures in place across technology, people, and process to minimise the impact and recover.



By focusing on cyber security alone and not extending this to cyber resilience, organisations are susceptible to higher risk. Ransomware payments are on the rise globally and unfortunately for the UK, we exceed the global average[3].

Section 2

Why Cyber Resilience is the New Organisational Minimum Standard

Cyber Insurance

Typically, to qualify for cyber business insurance organisations will need to prove that they utilise modern anti-virus, have data backups, identify software vulnerabilities, and patch them (vulnerability management), 24 x 7 managed threat detection and security awareness training. Some providers will also ask for security incident and event management (SIEM) and log retention.

Modern Threat Landscape

The methods used by cyber criminals are continually evolving and there's been a significant increase in the number of supply chain third party attacks over the last 3 years. Zero-day attacks that exploit vulnerabilities that do not have a fix in place are increasingly common. Networks have become more complex over time and mobile devices and the Internet of Things (IOT) have opened additional areas of vulnerabilities to exploit.

Rise In Hybrid/Remote Workforce

Whilst there are tangible benefits to many organisations of offering remote and hybrid working such as access to a wider talent pool and increased staff satisfaction, it also introduces additional cyber risk. These include increasing the complexity of connectivity and infrastructure, the use of more vulnerable public networks and a reliance on employees being cyber aware.

Increasing Compliance and Regulatory Requirements

As advancements in technology greatly outpace the speed of legal reform there has been a renewed push in recent times for international governments to take a hardened stance to cybercrime.
The increase in regulatory requirements and their complexity is demonstrated in the impending updates to the Network and Information Systems Regulations (2018), UK General Data Protection Regulation (GDPR), Product Security and Telecommunications Infrastructure Act (2022), UK government's proposed introduction of "cyber duty to protect", UK government's proposed strengthening of corporate responsibility to include a "Resilience Statement" in annual reports, proposed United Nations International Cybercrime Treaty.

This is why Outbound Group have decided to embark on a mission to educate organisations in the UK on what Cyber Resilience is and to partner with them on their strategy to achieve it.

outbound™ VIRTUAL

Section 3

Understanding the 5 pillars of Cyber Resilience

Identify

Start by picturing what valuables you need to protect most in your home. What things in your home are you most concerned about protecting? If you're like most people, you are probably thinking about your family, pets, personal documents, heirlooms, and technology devices.

Now, let's consider the same when evaluating your business. What data in your organisation is crucial in ensuring business continuity? It could be customer information, financial and operational data, intellectual property, and more.

Understanding what data you need to protect, is the first step in implementing the right technology solutions for your business.

Protect

Now, shift your mindset to think about how you protect those valuable items in your home. Do you protect your valuables with doors, windows, and locks? Maybe you have a fence or a security system to deter intruders.

So, how do you protect your organisation's data? You may need firewalls, encryption, multi-factor authentication, and employee cybersecurity awareness training.

Detect

You probably have multiple methods to detect if an intruder is in or around your home. You may have an alarm system, doorbell camera, or are a part of your local neighbourhood watch.

Yet, detecting an intruder in your organisation's environment is a bit more challenging. Depending on your industry and organisation, you may need a Security Operations Centre (SOC), end point detection & response (EDR), managed detection & response (MDR) or information and event management (SIEM).

Respond

If an intruder were to enter your home, how would you respond? You'd likely call the police, potentially use a baseball bat, or call your guard dog to defend yourself.

But how would you respond to a hacker accessing your organisation's data? It'd certainly be hard to deter a cybercriminal with a baseball bat! This is where you need to consider whether you can cover all bases, 24x7x365 quickly enough to contain damage and to initiate recovery in house. If not, consider extending coverage via strategic IT security partnerships to extend coverage out of hours, add additional resources or speed up your response time.

Recover

How would you recover from a break-in or bad storm at your home? I bet your insurance company would be getting a call. Maybe you would reinforce your house with flood defences or stronger locks.

But what happens if your organisation's data is held for ransom, or you experience a systems failure? You would need to enact your business continuity plan and utilise your backup solutions.

Ultimately, cybersecurity frameworks and cyber resilience makes one thing very clear: **having comprehensive, integrated cybersecurity and business continuity and disaster recovery (Disaster-Recovery-as-a-Service) solutions are instrumental in protecting and recovering your business's critical data.**

Section 4

Solutions - Help Is At Hand

We've covered a lot of ground and you're probably wondering, how on earth can anyone keep on top of all the parts of cyber resilience and bring the technology, people and processes required to achieve cyber resilience together?

The answer is honestly, not well and with great difficulty. That's why it is important to build a culture of cyber security being everyone's responsibility and selecting the right partnerships if you do not have all the knowledge in house to build out a full security practice.

Since inception, Outbound Group has focused on embedding cyber security into everything that we do.

Based on the wealth of experience the team has, a solid foundation of established partnerships with industry leaders in cyber security and cyber resilience, and our responsibility for IT systems and security across multiple geographies and industries we have put together four Cyber Resilience as a Service packages.

Our Cyber Resilience services are designed to be customised to suit your requirements, infrastructure, strategy and people. The Outbound team are well prepared to help yours whatever stage of your cyber resilience journey you are on.

outbound™ VIRTUAL

Section 5

References

[1] IDC: The premier global market intelligence company. (2023). New IDC Spending Guide Forecasts Worldwide Security Investments Will Grow 12.1% in 2023 to $219 Billion. [online] Available at: https://www.idc.com/getdoc.jsp?containerId=prUS50498423#:~:text=New%20IDC%20Spending%20Guide%20Forecasts

[2] GOV.UK. (n.d.). Cyber security breaches survey 2023. [online] Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023.

[3]The State of Ransomware 2023 Findings from an independent, vendor-agnostic survey of 3,000 leaders responsible for IT/cybersecurity across 14 countries. (2023). Available at: https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf
.

outbound™ VIRTUAL

www.outbound.group

Part of the outbound™ GROUP

Get in touch
Tel: +44 (0)207 183 1443
Email: sales@outbound.group