babble

THE BABBLE GUIDE TO CYBER SECURITY FOR SMBs →

2023/24

Babble E—book.

CONTENTS

The Babble Guide to ***Cyber Security for SMBs***

Today, small and medium-sized businesses (SMBs) in the UK face increasing cyber security threats. **The Babble Guide to Cyber Security for SMBs** is a straightforward e-book that provides the essential knowledge and strategies needed to protect your digital assets. In a landscape where data is invaluable and cyber attacks are proliferating, we're here to help you assess your own cyber risk and prevent breaches.

Why Read This Guide?

UK-Centric Focus: Tailored specifically for UK SMBs, the guide addresses the unique challenges and regulatory landscape of the region.

Actionable Insights: Instead of dense technical jargon, the guide delivers practical inights that SMBs can capitalise on for a more robust security posture.

Threat Landscape Awareness: Stay informed about the current cyber threat landscape, covering everything from common phishing scams, to emerging trends such as AI-assisted attacks.

Cost-Effective Strategies: This guide offers cost-effective cybersecurity strategies, helping SMBs prioritise investments wisely within budget constraints.

What Makes an SMB an Ideal Target?

Major enterprises might seem like the obvious choice for cyber attacks because of the vast amount of valuable and sensitive data they hold. Undoubtedly, the consequences of disruption are bigger for large enterprises. However, SMBs typically have more vulnerabilities, and their data is just as valuable to cyber criminals.

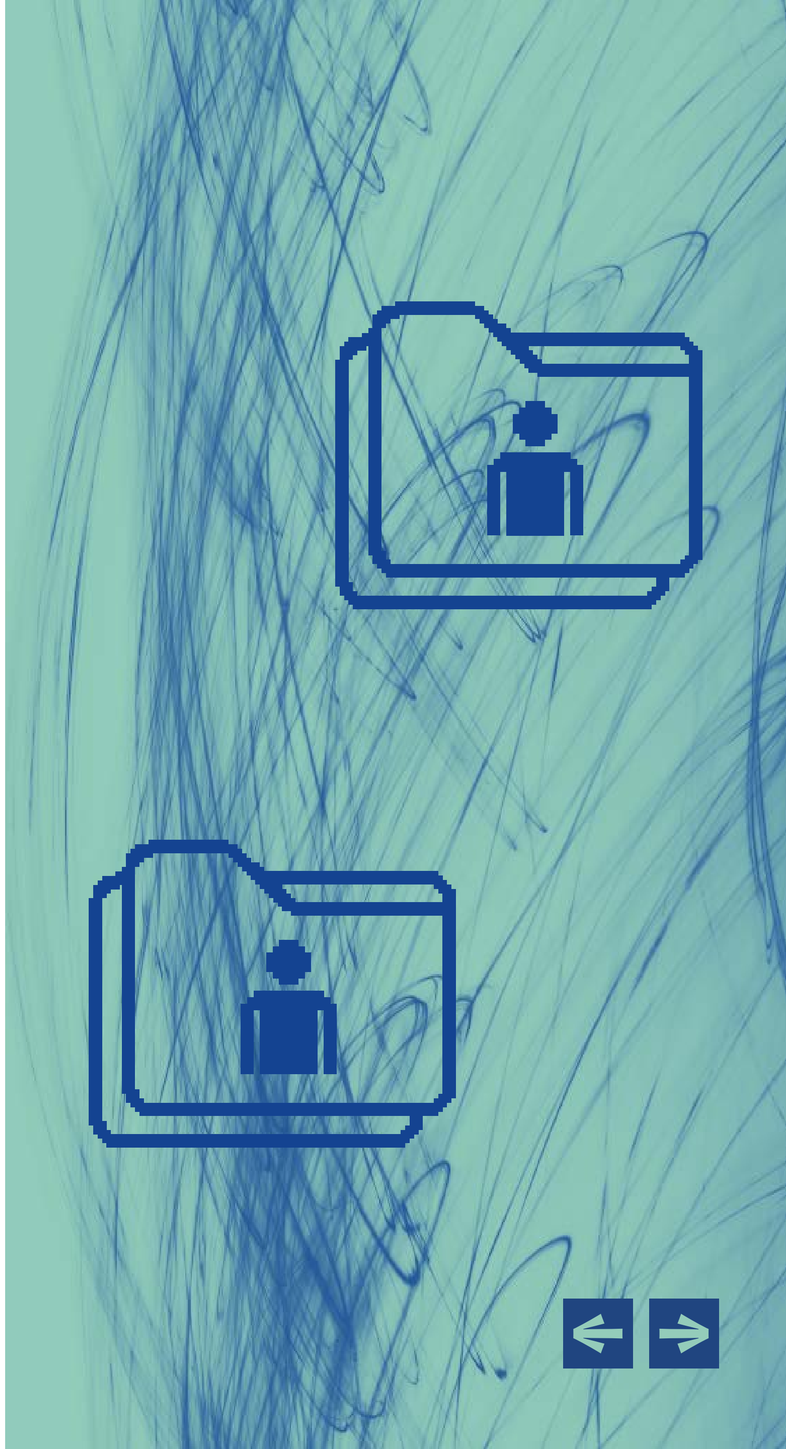
Large organisations that experience breaches often make news headlines but that doesn't mean that small and medium-sized businesses don't also experience breaches. SMBs are always at risk from a cyber attack. This is mainly because an SMB often lacks the cyber security team, tools, and resources needed to combat a modern cyber attack.

Both large enterprises and SMBs hold a treasure-trove of sensitive data, including employee and customer records, intellectual property, and financial transaction information. The difference between them lies in their ability to protect those valuable resources.

This ultimately makes SMBs vulnerable to ever-evolving threats and an easy target for criminal organisations.

"It's a common and dangerous misconception that cyber crime only affects larger businesses - unfortunately all the data shows that cyber criminals go where it's easiest for them to make a successful attack, and this means it its vital for all organisations, regardless of size, to take effective precautions."

– Charles Aylwin, Managing Director of Babble Tech



The Cost of Cyber Crime for SMBs

From ransomware and phishing attacks to the theft of sensitive data, cyber attacks can take many forms to access that valuable information.

A cyber attack is a reality for any business that can result in significant consequences such as financial loss, reputational damage, political implications and more.

“It is so important to make sure your organisation isn’t flagged as an easy target on Cyber Crime Target Lists - if you haven’t done a recent security audit, get one done and act on their advice. In the meantime, do the basics such as turning on Multi-Factor Authentication - this stops the vast majority of credential theft breaches. Don’t put off implementing the latest software patches, and replace obsolete operating systems - this reduces the “easy” ways in for criminals, and makes it more likely they’ll target a different organisation.”

– Charles Aylwin, Managing Director of Babble Tech

84%

84% of private sector organisations hit by ransomware reported that the attack caused them to lose business and revenue (Crowdstrike, 2022).

37%

Only 37% of businesses feel confident in their ability to remain resilient through a worst-case cyber event (Crowdstrike, 2022).

43%

43% of cyber attacks are aimed at small businesses, but only 14% are prepared to defend themselves (Mclean, 2023).

1. Crowdstrike (2022). Small Business Cyber security Survival Guide. Crowdstrike. Available here.
2. Mclean, M. (2023). 2021 Must-Know Cyber Attack Statistics and Trends - Embroker. [online] Embroker. Available here.

Cyber criminals use a variety of techniques to gain access to systems and valuable data. Let's take a look at the most common cyber attacks impacting businesses globally today:

Malware:

These malicious programs can take many forms, including viruses, worms, trojans, ransomware, and spyware. They aim to damage or disable computer systems, networks, or data.

Phishing:

Commonly email-based, phishing attacks attempt to trick victims into revealing sensitive information and credentials by impersonating credible people or organisations.

Malware-free Attacks:

Cyber attacks that don't always involve the use of malware. These fileless attacks use native, legitimate tools that are already built into systems to allow attackers to compromise existing environments.

Insider Threats:

Cyber attacks carried out by current or former employees, knowingly or not, can exploit computer systems or data. These threats can be difficult to detect and prevent and can have a devastating effect.

Compromised Credentials:

Using leaked or stolen login credentials, cyber criminals gain unauthorised access to computer systems, networks, and data, allowing them to perform various attacks masked as legitimate users.

Vulnerabilities:

Weaknesses in software, hardware, or networks that can be exploited by cyber criminals. Vulnerabilities can be caused by bugs in software, misconfigured systems, or outdated software.

Zero-days:

Attackers frequently exploit unknown and undetected vulnerabilities in software or hardware before developers can find a fix or release patches to address them. These vulnerabilities are often targeted with planned attacks.

Why Legacy Security Technology is a Liability in the Age of Modern Cyber Attacks

Most small businesses are familiar with the most common forms of cyber attacks like malware and have decided to combat them by simply installing antivirus. Although this approach may work against some attacks, cyber criminals are now adapting their tactics to become more advanced. They are abandoning traditional malware-based attacks in order to get around legacy antivirus software.

This has resulted in a surge of malware-free attacks, especially phishing and AI attacks. This can be seen in reports from the Ponemon Institute where they estimate that fileless attacks are more than 10 times more likely to succeed (Ponemon, 2018).

Fileless attacks are increasingly effective at evading detection; as a consequence, the trend is bound to increase. These attacks use legitimate tools or scripts to execute malicious commands in memory, without leaving any trace on the disk.

This makes it harder to detect and block by traditional antivirus software, which relies on signatures or heuristics to identify malware. They do not write any malicious files to the disk, so they cannot be detected by traditional antivirus software – one of the most common ways they present themselves is in phishing scams.

Ponemon Institute. (2018). The 2017 State of Endpoint Security Risk Report. [online] Available here.

[continued]

In addition, this form of attack can be used to deliver a variety of different types of malware, including trojans, ransomware, and spyware. This makes them a very versatile and dangerous threat.

As cyber criminals are finding new, harder to detect ways of accessing systems and infrastructure, they will be able to use valuable data in the following ways:

- **Data theft**: Through unauthorised acquisition, criminals extract and sell valuable sensitive data or intellectual property.
- **Ransomware**: By encrypting data and disabling access through malware, criminals are able to demand a ransom payment in exchange for the decryption key.
- **Extortion**: Instead of simply locking businesses out of the system, attackers can threaten to expose sensitive information publicly unless an extortion payment is paid.
- **Hacktivism**: Often used to promote an agenda or social cause, hacktivism is used to help gain visibility, publicity, and momentum.

"There are cyber criminal organisations whose sole purpose is to compile and market lists of companies who are vulnerable to different types of attack - this will include, details of out-of-date software, unpatched and obsolete operating systems, password lists etc. These lists are bought by other criminal entities who will use them to execute attacks, using Ransomware as a Service (RaaS - yes, its really a thing !) bought from thousands of specialist criminal organisations who write malicious code."

– Charles Aylwin, Managing Director of Babble Tech

The Role of Artificial Intelligence

In the past, traditional ransomware attacks often relied on mass distribution and brute-force methods, but the advent of artificial intelligence (AI) is revolutionising the ransomware landscape, making attacks more sophisticated, targeted, and impactful.

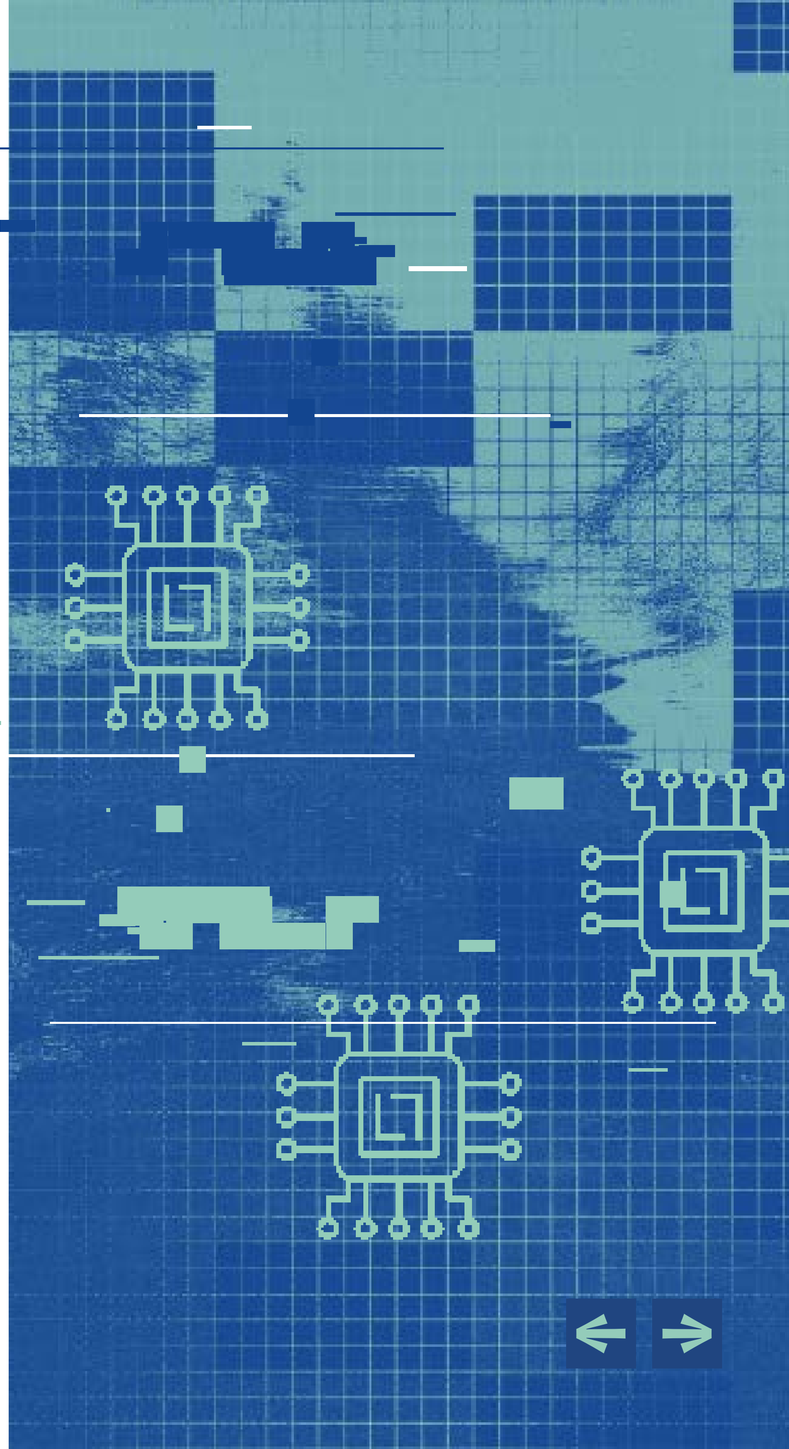
Here are some key ways criminals are using AI to orchestrate their attacks:

AI-powered Reconnaissance and Targeting:

AI enables criminals to enhance their reconnaissance and target selection strategies. Through the use of AI algorithms, attackers can analyse large datasets to identify potential victims based on vulnerabilities, financial status, and susceptibility to extortion. This targeted approach allows them to focus on high-value targets, maximising their potential returns.

Automated Attack Delivery and Execution:

AI is revolutionising the attack delivery process as well. With the help of AI-powered tools, tasks like phishing email campaigns, social engineering tactics, and vulnerability scanning can be automated. This automation empowers attackers to launch their assaults more swiftly and effectively, significantly boosting their chances of success.



[continued]

Security Defense Evasion:

The threat of ransomware attacks is amplified by the use of AI. Through advanced algorithms, AI can analyse network traffic, identify patterns, and cleverly adapt to bypass conventional security measures. As a result, organisations are faced with heightened difficulties in both detecting and preventing ransomware attacks.

Enhanced Encryption and Data Masking:

AI is further complicating the recovery of encrypted data. AI-powered tools can generate stronger encryption algorithms and utilise techniques such as data masking to make decryption more difficult. This increases the pressure on victims to pay the ransom.

AI-driven Ransom Negotiation

AI is even influencing ransom negotiation tactics. Algorithms can analyse victim behaviour, assess their financial capabilities, and optimise ransom demands accordingly. This personalisation makes it more difficult for victims to negotiate a lower ransom.

"With the ever-growing and ever-evolving threat of cyber attacks, cyber security for all businesses is a critical area that needs to be front of mind to ensure they are fully protected. With the addition of the AI revolution, we must be certain that our data cannot be compromised and if the worse does happen, we understand how we can restore the potential loss."

- James Faver, Babble Sales Manager

Four Cyber Security Steps *Every Small Business Needs to Take*

Step One:

Understand the Facts of a Cyber Attack

Myth: Cyber attacks are carried out by amateur hackers.

Fact: Cyber criminals are highly organised and skilled individuals who are motivated by financial gain or other malicious intent. They are constantly developing new and sophisticated techniques to exploit vulnerabilities and steal data.

Myth: I will know immediately if my business is breached.

Fact: It can take weeks, months, or even years for a business to discover that it has been breached. Cyber criminals are skilled at hiding their activity and covering their tracks enabling them to do more damage the longer they have access.

Myth: Small businesses are not at risk of cyber attacks.

Fact: Small businesses are just as vulnerable to cyber attacks as large businesses. In fact, they are even more exposed, given their limited resources and lack of expertise to implement robust security measures.

Myth: My business will recover from a cyber attack.

Fact: Recovering from a cyber attack can be costly and time-consuming. In some cases, businesses may never fully recover.

Myth: Antivirus and a firewall are sufficient to protect my business from cyber attacks.

Fact: While antivirus and firewall software are important security tools, they are not enough to protect against all types of attacks. New sophistacated techniques are constantly being developed to evade these traditional security measures.

Step Two:

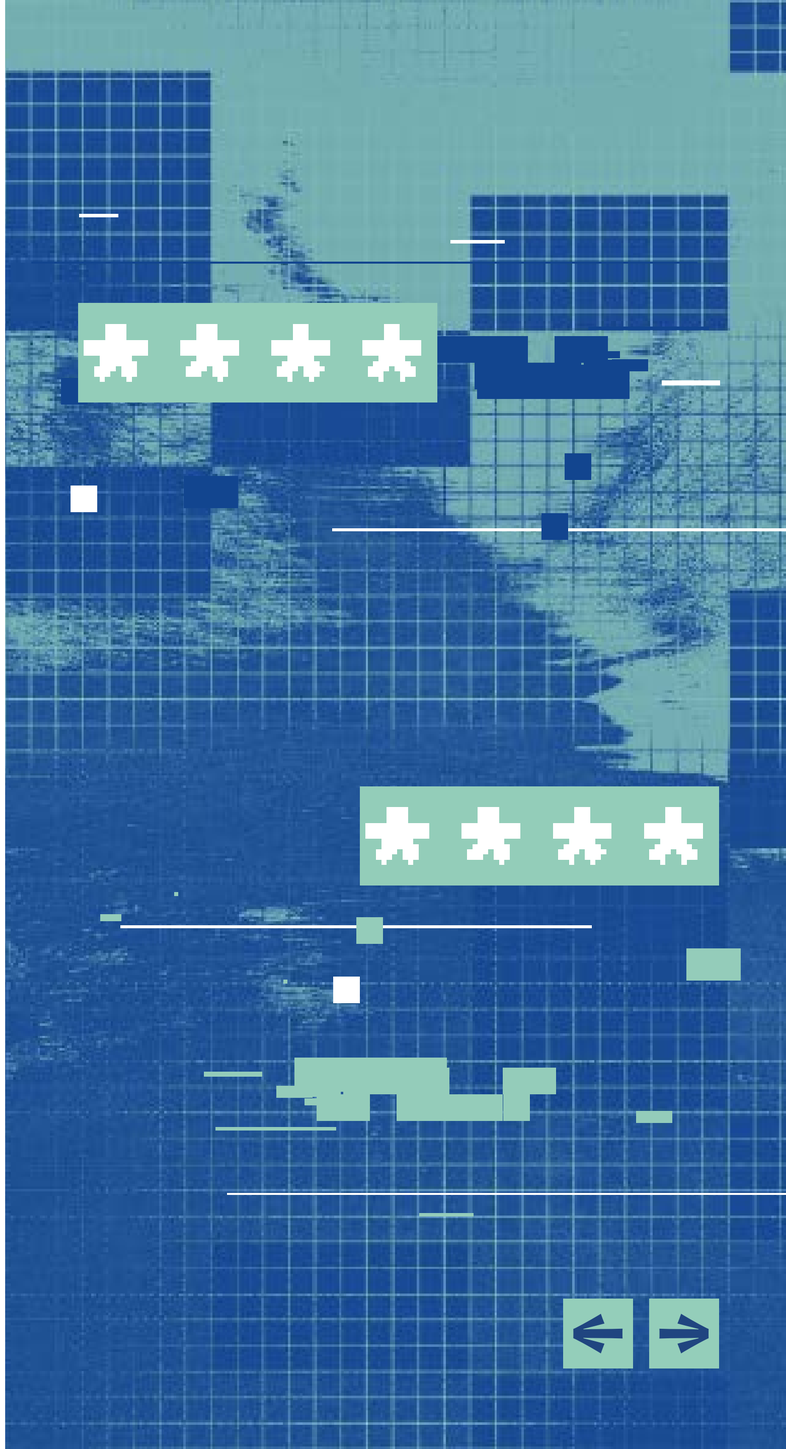
Employ the Fundamentals of Cyber Security

- **Enforce a strong password policy**: Passwords should never be shared or used for multiple accounts across apps or servers. Additionally creating an effective password management system allows businesses to find suspicious behaviour more efficiently.

- **Implement multi-factor authentication (MFA)**: A password alone is not enough to deter cyber criminals. MFA adds an extra layer of security by requiring more than just a password as evidence to log in. For example, that additional factor could be a physical security token, a biometric, or a one-time passcode (OTP) on an app, or sent to one's phone or email.

- **Back up critical data regularly**: In the event of a data breach or another disaster, backups, whether using cloud or on-premises, will help enable businesses to recover their data quickly. And while it's also important to ensure that backups are made regularly, it's also important to encrypt them.

- **Keep software up to date**: One of the most common forms of attack occurs when known vulnerabilities in software are exploited. Software updates often include securitypatches that fix known vulnerabilities. By keeping your software up to date,

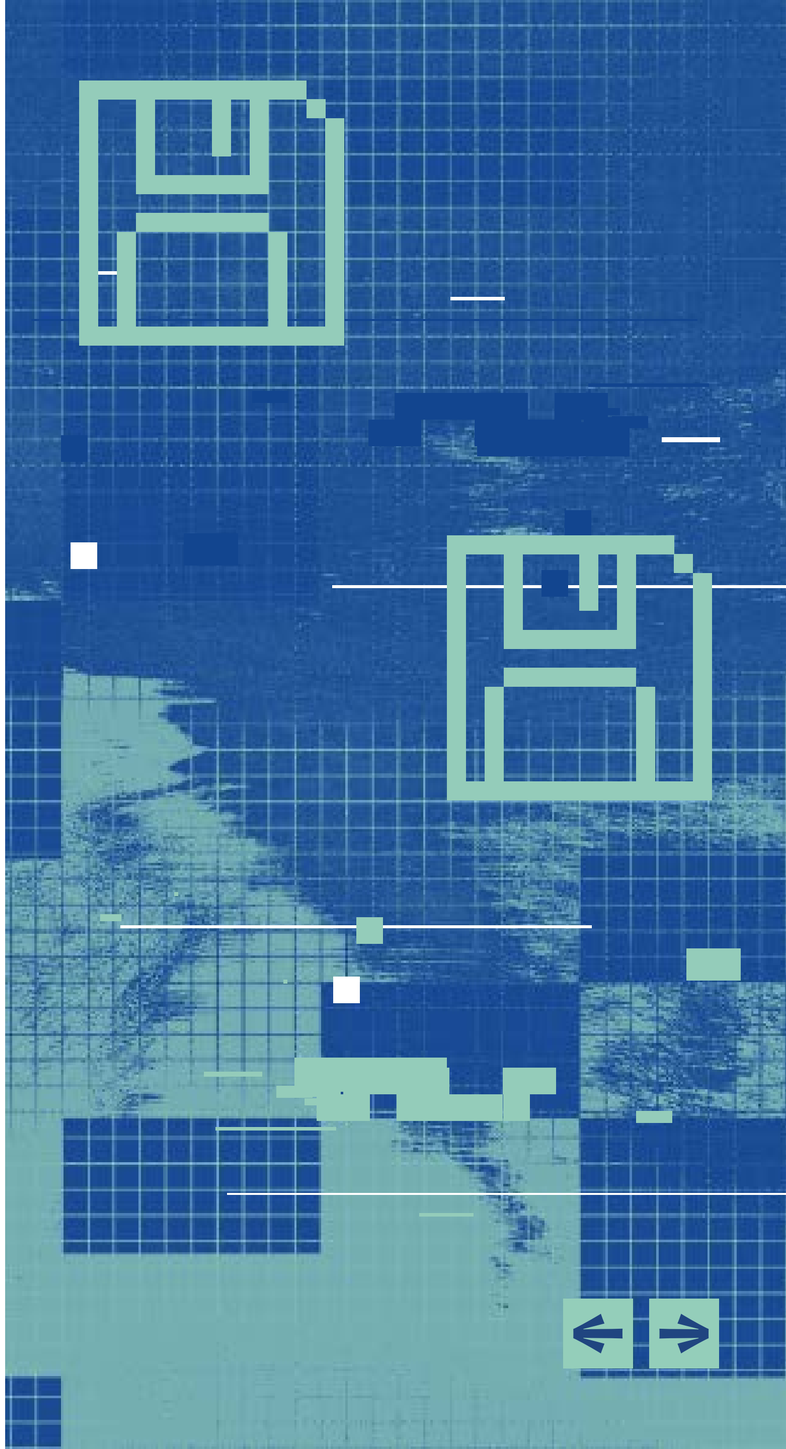


[continued]

- **Utilise the principle of least privilege**: Implementing the principle of least privilege is crucial for data security. It ensures employees have access to specific resources necessary for their job responsibilities, minimising the risk of unauthorised access, breaches, and internal threats. This measure safeguards sensitive information and maintains a robust security framework.
- **Implement and test threat detection and response**: A sufficient plan should include procedures for identifying, containing, and recovering from cyber attacks. It's important to test your plan regularly to make sure it's effective.
- **Secure the network**: Creating a private VPN and keeping Wi-Fi secure and hidden will ensure remote employees and networks are protected. This will also make it easier to find suspicious behaviour and access points which need to be addressed.

"It's a sobering fact that the vast majority of security breaches are a result of user error - depending on which survey you read, between 87-92% of are as a result of compromised user credentials. In plain English, this means that hackers aren't breaking in, they're logging in."

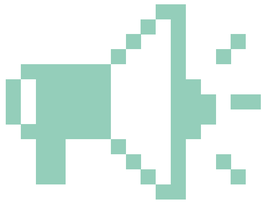
– Charles Aylwin, Managing Director of Babble Tech



Step Three:

Implement Cyber Security Awareness Training for Employees

Creating a culture of cyber awareness through employee training and testing makes a difference. According to Cisco's latest report, SMBs who fostered a culture of security saw a 46% increase in resilience in the overall environment (Cisco Secure, 2022).



Educating Employees:

Educating employees means ensuring that each individual in the workforce is made aware of each type of potential security threat and attack that they could face. Examples of these attacks include phishing, smishing, honey trapping, and more. Each of these attacks are tactics used to trick individuals into revealing valuable information, such as account credentials.

Continuously Test Employees:

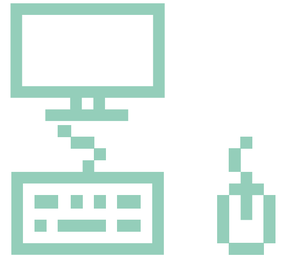
Keep your employees sharp by regularly testing their awareness training. It's crucial they stay up to date and know how to spot attacks in real-world scenarios. Evaluating an employee's ability to identify potential threats will help identify who needs further training, guidance, and information.

Cisco Secure (2022). Security Outcomes Report Volume 3. [online] Cisco. Cisco. Available here.

Step Four:

Understand The Importance Of Modern Endpoint Protection

Endpoint protection should be a key consideration when looking for a modern security solution. One option worth investing in is endpoint detection and response (EDR) software. It will ensure the protection of computers, mobile devices, servers, and other connected devices, from both known and unknown threats and vulnerabilities.



EDR offers a variety of security benefits, including:

Real-Time, End-to-End Visibility:

EDR provides a comprehensive view of your security posture, including all devices and applications, in real-time. This can help you to identify and respond to threats quickly and effectively.

Improved Threat Detection and Resolution:

EDR uses advanced technologies to detect and block a wide range of threats, including malware, ransomware, and phishing attacks. EDR can also help automate the investigation and remediation of threats, saving you time and resources.

Enhanced Efficiency and Improved Outcomes:

EDR can help you streamline your security operations and improve your overall security posture, leading to reduced costs and improved business outcomes.

EDR is an essential component of any cyber security strategy for businesses of all sizes. It can help you to prevent data breaches, protect your customers and employees, and comply with industry regulations.

[continued]

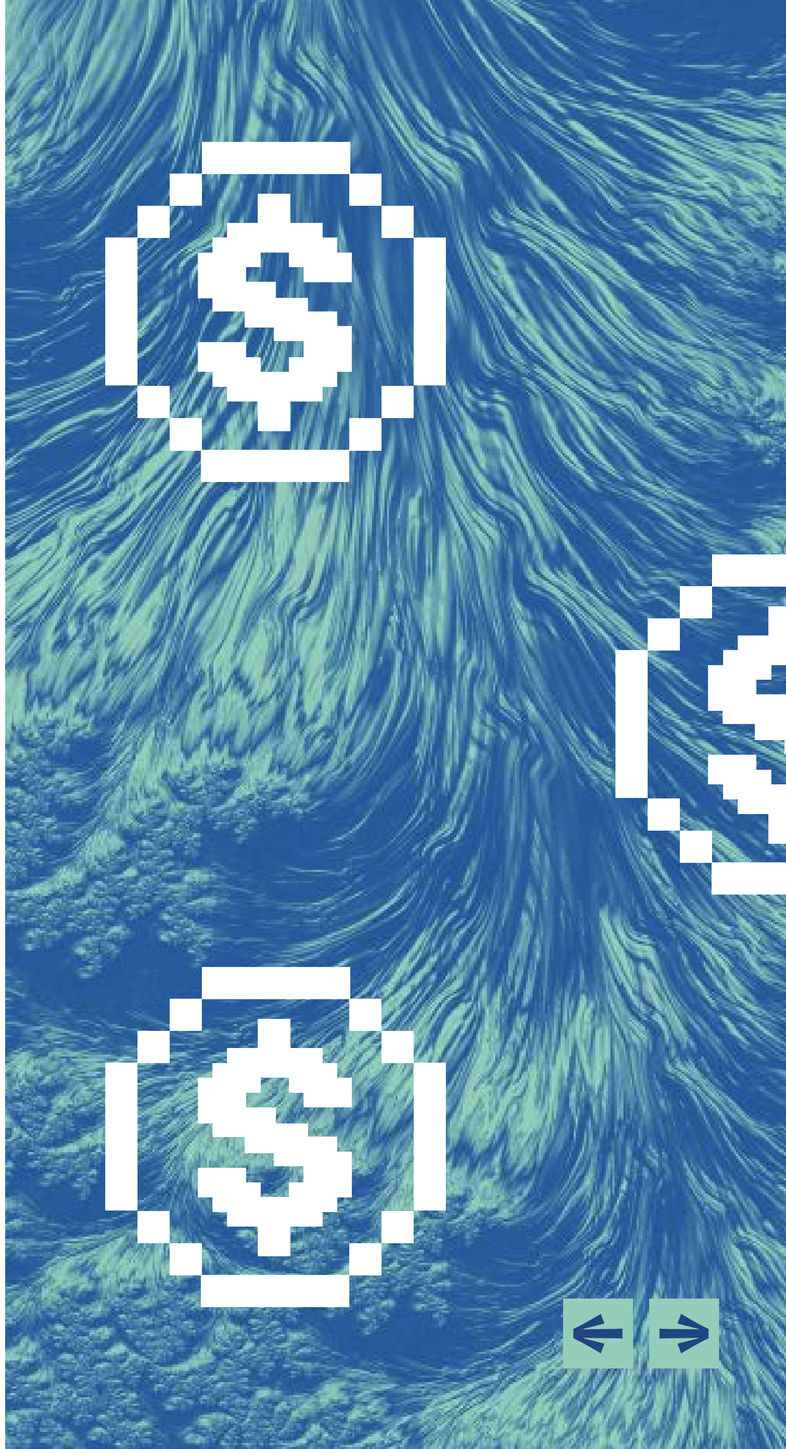
Resources and Expertise on a Budget

While an EDR solution is effective for proactive protection, it may not be an ideal option for those who lack the budget or time to implement it. It needs a dedicated team capable of setting policies, monitoring for attacks, and responding to and stopping them.

If your business is in this scenario, then a managed detection and response (MDR) solution may be the best fit. MDR is a cyber security service that uses technology and human expertise to find, monitor and respond to threats.

MDR services can be a valuable asset for a small business that doesn't have the resources or expertise to manage its own cyber security operations.

According to Gartner, by 2025, 50% of organisations will use MDR services for threat monitoring, detection, and response functions (Sophos, 2023).



Sophos (2023). The State of Ransomware 2023. Sophos. Available here.

Conclusion

Cyber security is absolutely crucial for SMBs in today's digital age but protecting your business requires a multi-faceted approach. From implementing multi-factor authentication to establishing robust threat detection and response plans, every step is vital to ensure your business's security.

But it doesn't stop there. Equipping your employees with cyber security awareness training is key to creating a secure work environment. Modern endpoint protection and managed detection and response solutions can further fortify your security framework, shielding your business from both known and unknown threats.

Even with budget constraints, there are effective solutions tailored for SMBs that strike the perfect balance between cost and security. Remember, in the realm of cyber security, prevention always trumps cure. With the right strategy and resources in place, SMBs can significantly enhance their resilience against cyber threats.

babble

Contact us

Interested in finding out more about Babble's work in the field of SMB cyber security?

Visit our website, or set up a call with one of our cyber security experts.

0800 440 2959