CYBER SECURITY PRIORITIES FOR SMBs

Benchmarking, best practice and practical advice

A July 2024 report by

DOHERTY ASSOCIATES

Combined Expertise

Table of contents

Introduction

In 2024, small to medium-sized businesses (SMBs) face unique challenges that can make it difficult to develop and maintain effective cyber security strategies. This eBook presents research from Doherty Associates on how UK SMB cyber security decision-makers are handling risks and vulnerabilities, and the challenges they face in doing so. It enables you to benchmark your organisation against peers, gain insights into Best practices, and access actionable advice to enhance your cyber security posture.

While the world of cyber security can be complex, this guide is designed to be accessible and practical. It focuses on essential areas that SMB leaders need to understand to get started or update their strategies, explaining key terms and concepts in plain English.

Each section of this eBook follows a clear, digestible structure to help you quickly absorb and apply the information:

- **Are you here?** - Benchmark your organisation against similar SMBs.
- **Best practice** - Advice on how to improve your cyber security measures.
- **If you only do one thing** - The best place to start in a time-poor world.
- **Next steps** - Key actions to take to enhance your cyber security.

We cover critical areas such as cyber security risk assessments, IT asset management, third-party risk management, threat intelligence, incident response, security awareness training, and the use of advanced security tools. Our research highlights key trends and challenges, providing you with a comprehensive view of the current SMB cyber security landscape.
For instance, our findings reveal that while many SMBs are conducting regular risk assessments, there's room for improvement in frequency and expertise. We also uncover gaps in areas like third-party risk management and the identification and remediation of critical vulnerabilities.

Whether you're just starting to develop your cyber security strategy or looking to enhance existing measures, this eBook provides the guidance you need to protect your business from evolving cyber threats. By understanding and addressing these critical areas, you can significantly improve your organisation's cyber security resilience.

Executive summary

As part of our ongoing commitment to supporting small to medium-sized businesses with their security posture, Doherty Associates conducted research to understand the current state of cyber security practices and challenges faced by UK SMBs.

The research

The research was conducted in June 2024. The survey panel comprised 309 cyber security decision-makers working in UK SMBs across various industries.

KEY FINDINGS

- **64%** conduct formal cyber security risk assessments quarterly or monthly
- **30%** cite lack of in-house expertise as the biggest challenge in risk assessments
- **65%** observed increased staff awareness from vulnerability scans
- **25%** manage IT asset inventories manually with audits
- **22%** continuously monitor third-party security practices
- **49%** use threat intelligence for proactive security measures
- **30%** have fully implemented and regularly updated incident response plans
- **62%** use online modules for security awareness training
- **57%** use EDR solutions for detecting suspicious activity
- **24%** do not use CASB solutions to secure cloud traffic

Executive take away

The cyber landscape has shifted rapidly in recent times. In response to a world of increasingly sophisticated cyber-attacks, many SMBs have taken important steps forward to bolster their cyber defences. Yet, across the thirteen essential areas covered in this eBook, our research shows that many SMBs remain inadequately prepared to handle the latest threats.

Many security teams are over-stretched or struggling with a lack of expertise and are taking essential protective actions with insufficient frequency. In some cases, cyber security strategies lack the required depth, and the implementation of critical security tools is incomplete. To achieve a requisite level of cyber resilience, it is crucial for SMBs to consider the improved practices, regular assessments, and adoption of advanced security solutions outlined in this eBook.

Risk assessments

A risk assessment is the very first step you should take with your cyber security strategy. It helps you work out the types of risk your business is vulnerable to, where breaches or attacks are most likely to come from, what impact these could have on your business, and how to start protecting against them. Those risks most often include compromised customer data, interrupted operations, or financial losses from fraud.

Risk assessments are particularly essential for small business leaders who may not have formal risk management processes in place and need to build their cyber security strategy from scratch.

From our research

17% of SMBs reported that they run risk assessments on an annual basis

33% on a quarterly basis

3% only don't run any risk assessments at all

So, if a good risk assessment saves you trouble down the road and prevents breaches from cutting into your profits, your customer loyalty, or your license to operate, why do some firms not prioritise them?

Are you here?

As we've seen, it's surprisingly common for smaller firms to not carry out formal risk assessments. In the finance and insurance sectors, 73% of firms treat cyber security as a very high priority vs 36% of all businesses. These other companies may not think they're large enough to be targeted, it will be too complex, or it will cost them too much money. This is why 36% of firms who carry out risk assessments only use internal staff, often not offering them the additional support they need.[i]

Our data shows that, for respondents who haven't carried out a risk assessment yet, these are the top 3 reasons:

- Lack of in-house expertise (30%)
- Competing priorities within the organisation (23%)
- Insufficient budget or resources (22%)

Risk assessments are remarkably straightforward with the right approach. However, without one, these firms' security decisions and safeguards will be fragile, often based on instinct, individuals' past experiences, or ad-hoc reactions to circumstances as they arise.

Best practice

Firms are increasingly recognising the importance of a more structured – though still straightforward – risk assessment process. It begins by identifying your critical data, systems, and processes. Then, evaluating threats that could disrupt them and looking at how you can prevent or detect these incidents through employee training, access controls, encryption, and other safeguards.

A modern, forward-looking, and robust risk assessment is proactive and involves a lightweight review of assets, controls, vulnerabilities, and threat landscape. It allows you to quickly adapt to new challenges, prepare to quickly notify your customers about a breach, and plan a response to save your reputation, customers, and ultimately revenue. For instance, if you're prepared for a data breach – often caused as a result of insider threats, third-party vendors, or social engineering – you can give your company a way to sidestep the reputation and financial costs associated with recovery.

[i] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

KEY SECTIONS OF A RISK ASSESSMENT:

Scope: Define the scope and boundaries of what the risk assessment will cover.

Risk identification: Brainstorm risks, review incident history, and learn from others' experiences.

Risk analysis: Estimate the likelihood it will occur and potential impact.

Risk evaluation: Evaluate which risks need treatment and priority using the results of risk analysis. Risks above a certain threshold need to be addressed.

Risk treatment: For priority risks, define mitigation actions, solutions or controls to reduce likelihood or impact. Assign responsibility, resources, timelines.

Monitoring and review: Put processes in place to monitor risks and review/update the risk assessment periodically. New risks may emerge over time requiring reassessment.

Communication and consultation: Communicate key risks and treatments to stakeholders. Consult them for input into the risk assessment.

Since 30% of SMBs cited lack of in-house expertise as their primary challenge in running regular and formal risk assessments, many businesses consult with a Managed Security Services Provider (MSSP) to help plan a strong foundation for their cyber security strategy.

If you only do one thing...

Informally identify the potential risks facing your business. If you need to, open a spreadsheet and brainstorm your main concerns, both internally and externally, and what effect these risks might have on your business.

Only 13 % of businesses say that they review the risks posed by their immediate suppliers.[ii] So, you can get ahead of your competitors with one move: look at your dependencies. If a third-party payroll provider shut down unexpectedly or a cloud provider outage prevented access to files, how would that affect your daily operations? For each risk, you want to capture the likelihood of it happening, as well as the impact if it does. Score all your risks that way, and you now have a metric by which to prioritise which ones come first when it comes to creating treatment plans.

Next steps

Develop a simple risk management plan and review it regularly to move towards the full risk assessment process outlined above. Work out the potential business impacts from incidents like data theft, ransomware, or service outages to prioritise security investments that offer the best protection against threats posing the greatest risk.

Share this plan with internal stakeholders to keep everybody on the same page – explaining the operational or business reasons behind the processes you're putting in place. UK Government statistics show that 65% of medium businesses update their senior team on cybersecurity strategies at least quarterly. It's crucial to treat this plan as a living document, not a set of commandments. In addition to these regular, scheduled reviews, put in dedicated meetings to revise the document when your business makes a significant change or external conditions change.

Alex Bransome
Chief Information Security Officer
Doherty Associates

However, you don't know what you don't know. If you're not a cyber specialist, it may be worth getting external assistance to map out your risk landscape.

[ii] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023

Vulnerability management

Vulnerability management is a systematic approach to managing cybersecurity risks associated with the weaknesses in your digital environment. It involves identifying, classifying, prioritising, and mitigating vulnerabilities before attackers can exploit them.

It's like conducting regular health checks for your business's IT systems to find any weaknesses that could let hackers in. This process is vital: keeping your digital doors locked against people and software that shouldn't be there. For SMBs, vulnerability management is a crucial part of cybersecurity hygiene. With new software and threats emerging left and right, protecting your data and customer trust means having a strong understanding of where your systems might be vulnerable.

Caleb Mills
Professional Services Director
Doherty Associates

Essentially, vulnerability management means you're not just waiting to respond to an attack; you're actively looking for and fixing weak spots to prevent breaches from happening in the first place.

Are you here?

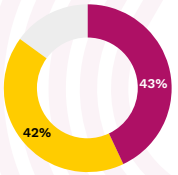
Our research shows that 6% of SMBs do not perform vulnerability scans at all. The focus is often on putting out fires or acting in retrospect - dealing with problems only when they directly impact the business, like after a cyberattack or data breach.

This reactive approach, however, can lead to downtime, loss of customer trust, and significant financial losses. For example, the importance of regular software updates may not be realised until after they've been hit by a ransomware attack that exploits an old, unpatched vulnerability.

To secure the best outcomes for your organisation, you can't always rely on past threats as a reliable indicator of what's to come. In recent years, cybercriminals have developed increasingly sophisticated automated tools that can scan the internet for vulnerable systems and launch attacks at scale, targeting all types of organisations, not just larger enterprises. These "exploit kits" make it easier than ever for even unskilled hackers to find and exploit known software vulnerabilities.

Best practice

As new software vulnerabilities and cyber threats continue to emerge, it is crucial to take the initiative when it comes to vulnerability management. This includes continuously scanning for vulnerabilities, assessing their potential impact, and addressing them according to their severity.



Our research shows that 43% of SMBs who run vulnerability scans were able to identify and remediate critical vulnerabilities in their systems, and 42% were able to improve compliance with industry standards.

Modern tools and services make it easier for SMBs to implement these processes, providing real-time insights into potential threats and automated ways to fix them before they cause harm. For example, adopting a vulnerability management program can help a business avoid a costly breach by identifying and patching a software flaw before it's exploited by cybercriminals.

A STRONG VULNERABILITY MANAGEMENT PROGRAMME IS A CONTINUOUS CYCLE WITH THE FOLLOWING STAGES:

- **Prework:** Determine the programme's scope, define roles and responsibilities, select vulnerability scanners, create and refine policy and Service Level Agreements (SLAs), and identify asset context sources.
- **Identify network assets:** Scan the network to identify all components such as devices, systems, and services that make up the network infrastructure.
- **Evaluate security posture:** Use the results from network scans to assess the overall security stance of the network.
- **Address findings:** Identify vulnerabilities from the security assessment and remediate them.
- **Report:** Document the vulnerabilities found and the actions taken to address them.
- **Prioritise:** Assess vulnerability value and add threat context.
- **Mitigate:** Remediate the vulnerabilities and accept the risk that cannot be remediated.
- **Reassess:** Rescan to validate remediation and adjust SLAs as necessary.
- **Improve:** Evolve your processes and SLAs and eliminate recurring issues.

A recent survey by the UK government found that **only 13% of businesses review the risks posed by their immediate suppliers.** Vulnerabilities in third-party software and services can have a devastating ripple effect, so if you want to get on the front foot with your cybersecurity efforts, make sure to institute comprehensive vulnerability management across your entire ecosystem.

If you only do one thing...

Start with a vulnerability assessment to understand your business's cybersecurity risks. Once you have that documented, go down the list and identify the most critical vulnerabilities that need immediate attention.

Once you have a clear picture of the weaknesses in your digital environment, this will naturally reveal the most pressing vulnerabilities that expose your business to the greatest risks, allowing you to prioritise your remediation efforts to allocate the most resources to the most effective actions.

Next steps

Develop a comprehensive vulnerability management programme. This should include regular scans, a process for prioritising vulnerabilities based on their risk, and a plan for timely remediation. Additionally, invest in employee training to raise awareness about the importance of cybersecurity Best practices, such as regular software and OS updates.

Asset inventories

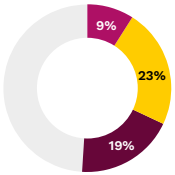
Understanding the technology that powers your business is the cornerstone of any robust cybersecurity strategy. Asset inventories serve as detailed records of all the technology - hardware and software - a business uses, helping you to manage them effectively.

For small and medium-sized businesses (SMBs) that may lack formal cybersecurity processes, maintaining an up-to-date asset inventory is crucial. It helps identify potential vulnerabilities and ensures consistent coverage of security policies and controls across all assets.

Without a proper asset inventory, businesses risk using outdated or unsupported hardware and software, increasing their exposure to cyber-attacks. For example, an unaccounted-for laptop containing sensitive information without disk encryption could be an easy target for thieves, leading to data breaches.

Are you here?

The approach to tracking IT assets in many SMBs can best be described as informal. Equipment and software are often procured on an as-needed basis, without a comprehensive system to track these assets.



Indeed, in our research, 9% of SMBs do not maintain an asset inventory, and the most cited challenges are budget constraints (23%) and lack of training (19%).

This lack of formal inventory management can lead to the continued use of outdated and unsupported technologies, significantly heightening the risk of cyber vulnerabilities. An unsupervised laptop loaded with sensitive data, for instance, is a data breach waiting to happen due to inadequate security measures.

Best practice

Forward-thinking SMBs today recognise the importance of developing and maintaining a detailed asset inventory. It's about more than just listing what hardware and software are in operation; it involves monitoring their security status to ensure everything is current and secure. This includes keeping tabs on software updates and knowing when technology reaches its end of life.

To streamline this process, many organisations turn to automated asset management solutions.

49%

From our research, 49% of respondents include some degree of automation – whether mostly automated or integrated into a hybrid approach – in their asset inventory process.

Automation tools come equipped with device discovery capabilities, which automatically identify and log new assets. This approach not only saves significant time but also reduces the risk of human error, ensuring no asset goes unnoticed.

Understanding your technological assets is fundamental to securing them. For instance, managing Citrix servers effectively requires knowledge of their presence and their current versions. After all, an asset inventory serves multiple purposes, from lifecycle management to enhancing security protocols.

There are several benefits to a detailed asset inventory; it allows you to:

- Identify and phase out vulnerable or obsolete technology through regular inventory reviews.
- Ensure consistent application of security policies and controls across all assets.
- Prioritise remediation activities to strengthen the overall security posture.

For example, after implementing an automated asset management system, you might discover several outdated software versions in use. This would help you to prioritise patching these vulnerabilities, avoiding potential cyber-attacks.

Today's asset inventories must reflect the expanded IT ecosystem, including cloud services and mobile devices. This broader scope ensures that all potential vectors for cyber threats are accounted for, from on-premises hardware to cloud-based applications and mobile technologies. This allows you to take a much more holistic view of your technology set-up.

When we consider that nearly a fifth (19%) of respondents marked lack of training as the biggest barrier to maintaining an accurate asset inventory we can see how vital it is to incorporate asset management into your broader security policies and training programs, ensuring everyone in your organisation understands their role in safeguarding your digital assets.

If you only do one thing...

Start by creating a detailed ledger of your technology assets. This means opening up a spreadsheet or using a basic database to record every piece of hardware and software your business relies on.

Make sure to note the version numbers and the expiry dates for any security support. This can serve as your first line of defence, giving you a bird's eye view of your technological landscape and helping pinpoint areas that might need immediate attention or updates. Keeping this inventory current is critical, so consider setting reminders for those important security-related dates.

Alex Bransome
Chief Information Security Officer
Doherty Associates

Fine-tuning your tech tracking isn't just about adding new tools - it's also about setting up the right internal procedures.

Next steps

To take your asset inventories to the next level, setup an automated asset management system. These systems are invaluable: not only automating the tracking and updating of your asset list but also actively identifying and flagging out-of-date software and potential vulnerabilities. This proactive stance allows you to prioritise security patches and updates effectively, ensuring your defences are as robust as possible.

Also, make sure to put together a set of internal procedures that will help you maintain the accuracy and relevance of your asset inventory. This should include regular reviews and updates to reflect any changes in your technology environment, such as new acquisitions or the retirement of old assets.

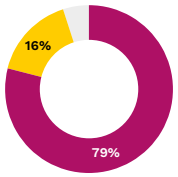
Third-party risk management (TPRM)

Third-party risk nanagement (TPRM) is an essential process for small to medium-sized businesses (SMBs) that rely on external vendors, including service providers and software developers. EY has found that 90% of organisations have directly invested in their TPRM programme, showing that many firms consider this a cornerstone of their cybersecurity strategy.[iii] First and foremost, a TPRM helps you to address risks that could transform essential third-party tools and services into liabilities.

TPRM is an evaluation process that looks at your potential risks in areas like data privacy, service delivery, software security, and compliance. It makes sure that the external components you rely on, those most integral to your daily operations, don't undermine your organisation's cybersecurity posture. For SMBs, resources are often limited, and this is where TPRM's structured approach to managing external risks effectively can make a difference.

Are you here?

Many organisations prioritise functionality and cost over security when adopting new software or services. However, given the additional risks introduced by third parties that may not adhere to security Best practices, this can cause its own set of problems. For instance, using cloud applications that do not meet stringent security requirements can open backdoors for data exfiltration.



Doherty Associates data shows that only 79% of SMBs assess the cyber security posture of third-party vendors. 16% admit they do not assess third-party vendors at all, indicating potential vulnerabilities in the supply chain.

Best practice

Adopting a mature approach to TPRM involves conducting thorough evaluations of service providers' security practices and the security features of the software being considered. This means looking beyond what the software does to understand the level of access it requires, how it manages and protects user data, and its compliance with relevant standards.

For organisations adopting a cloud storage solution, for instance, they might run an assessment of the provider's security measures. This includes evaluating their encryption methods, access controls, incident response plans, and compliance with industry standards such as ISO/IEC 27001. It might also assess the provider's policies on data sovereignty, considering where its data will be stored and how it will be protected under different jurisdictions' laws.

22%

Continuous monitoring is employed by 22% of businesses we surveyed, which showcases the proactive stance towards maintaining third-party security standards that many SMBs are moving towards.

Contracts with vendors could, for example, include stipulations about maintaining cybersecurity standards and regular security reporting. Many firms negotiate the right to audit clauses and, if possible, include breach notification clauses with specific timelines. It's crucial to define what constitutes a 'security incident' and the protocol for escalation and resolution. Penalties for non-compliance can also incentivise vendors to maintain robust security standards.

Forward-looking organisations will establish policies and procedures to prevent staff from signing up for unapproved or unverified applications, ensuring that any new software acquisition goes through a security vetting process. This can include implementing a whitelist of approved applications and regularly reviewing this list for any security or operational changes.

[iii] https://www.ey.com/en_gl/insights/risk/2023-ey-global-third-party-risk-management-survey

A robust TPRM strategy includes regular risk assessments and security audits of third-party vendors. This can leverage a tiered approach to risk assessment, focusing more intensive audits on higher-risk vendors. Given that a vendor's risk level can change over time, it's important to reassess regularly.

A cooperative relationship with vendors to explore and enhance security measures helps both parties' compliance efforts. It's more effective to work together towards compliance than to enforce it unilaterally.

If you only do one thing...

Identify your highest-risk third parties, focusing on those with extensive access to systems or those whose outage or breach would have a significant impact. Is it your payroll service provider, who manages employee financial information, or is it your legal services provider, whose access to sensitive case files and compliance documents could pose a significant risk if breached?

Next steps

Develop a TPRM security questionnaire for third-party providers to evaluate their cybersecurity measures and compliance with industry standards. Incorporate scenario-based questions to gauge their incident response capabilities.

Make sure the questionnaire is dynamic and can be updated as new threats emerge. It's not just about ticking boxes; it's about understanding the vendor's security culture and practices.

Threat intelligence

Threat intelligence is all about gathering and analysing information about emerging or existing threats and vulnerabilities that can impact your business. It's a proactive approach to news monitoring and information gathering that helps you stay one step ahead of potential cyber threats.

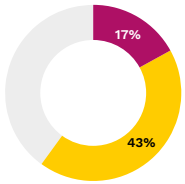
Just as you'd prepare for a storm by checking the forecast and securing windows and doors, threat intelligence helps you brace your digital environment against potential cyberattacks by informing you of the latest threats and how they can affect your business.

Cyber threats, much like real-life viruses, evolve and mutate so much that many companies will hardly have adapted to the last attack vector before a new one appears. Having up-to-date information means you can quickly adapt your defences to protect your critical assets. By embracing threat intelligence, you're not just reacting to attacks after they happen; you're preparing and preventing them, keeping business resilience at the top of your priorities.

Are you here?

Many businesses operate in a reactive mode, addressing cyber threats only after they have been impacted. Unfortunately, this approach can result in significant financial and reputational damage. For example, a company suffering a severe data breach might be unaware of a known vulnerability being exploited in the wild.

The lack of a proactive threat intelligence strategy can cause businesses to always be a step behind cybercriminals, leading to unnecessary exposure and increased risk of attack.



In our research, only 17% of SMBs say that they update their threat intelligence data in real-time or automatically, with 43% doing so on a daily, weekly, or monthly basis. This suggests many organisations may be operating with outdated threat intelligence, limiting their ability to stay ahead of rapidly evolving cyber threats.

Best practice

The key is to be proactive, stay informed, and learn about new threats rather than acting only after an incident has happened. By monitoring threat intelligence feeds, a business could learn about a new phishing or ransomware campaign targeting their industry and take steps to strengthen their defences before being attacked. This approach minimises the risk and impact of cyber threats on operations and customer trust.

Caleb Mills
Professional Services Director
Doherty Associates

The most successful companies subscribe to commercial threat feeds or join industry-specific information-sharing groups like Information Sharing and Analysis Centres (ISACs). These platforms provide a private forum where specifics of emerging threats are shared, enhancing all members' preparedness. They regularly check these threat intelligence feeds, akin to reading BBC News, to see what's coming down the pipeline and prepare accordingly.

These companies can stay one step ahead of the bad actors by integrating Indicators of Compromise (IOCs) into their SIEM systems. These IOCs are the fingerprints of attacks, enabling immediate detection of past and future attempts.

By incorporating threat intelligence into your cybersecurity strategy, you'll be able to anticipate and mitigate threats before they cause significant harm, keeping your operations running and your customer trust intact. Indeed, many organisations implement a process for regularly reviewing and updating their threat intelligence. Cyber threats are constantly evolving, and so your defences might need an update to stay effective.

Threat intelligence is also about understanding the motivations and tactics of cybercriminal groups targeting your industry. The most mature threat intelligence programs integrate data from a variety of sources, including dark web monitoring, open-source intelligence, and even industry-specific threat-sharing communities. You're not just collecting data but also analysing that data to uncover trends, indicators of compromise, and predictive signals that let you set up a defence in time.

41% of SMBs leverage threat intelligence to inform incident response processes like scoping attacks and identifying indicators of compromise. Interestingly, 32% also cite using threat intelligence to guide broader strategic decision-making beyond just security operations.

To get a wider view of the threat landscape, engaging with cybersecurity communities and forums can be valuable. A sector-focused outsourced security partner can often provide this capability, reducing the hassle and complexity of monitoring threat intelligence feeds or subscribing to an ISAC. They handle the information sharing and threat monitoring, offering additional insights and a better understanding of the cyber threat landscape relevant to your business sector.

TO IMPROVE YOUR THREAT INTELLIGENCE CAPABILITIES, CONSIDER JOINING ONE OF THESE TYPES OF INFORMATION-SHARING GROUPS:

Information Sharing and Analysis Centres (ISACs): Sector-specific communities that facilitate the sharing of cyber threat data, such as the National Cyber-Forensics and Training Alliance (NCFTA) and the Retail Cyber Intelligence Sharing Centre (R-CISC).

Information Sharing and Analysis Organizations (ISAOs): Voluntary, community-based groups that share threat intelligence, like the Cybersecurity Information Sharing Partnership (CiSP) in the UK.

Public-Private Partnerships: Collaborations between government agencies and private sector organizations, such as the UK's National Cyber Security Centre (NCSC) and the US Department of Homeland Security's Enhanced Cybersecurity Services (ECS) program.

If you only do one thing...

Start by subscribing to a basic threat intelligence feed tailored to your industry or partnering with a security provider with expertise in your industry. This is a simple step which can provide insights into the specific threats targeting businesses like yours, allowing you to make informed decisions about your cybersecurity defences.

Next steps

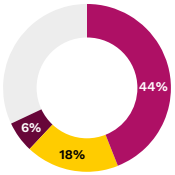
Develop a more sophisticated threat intelligence strategy. This could include setting up a dedicated team or function within your business to analyse threat data, integrating threat intelligence into your existing security tools for automated defence adjustments, and conducting regular training for your staff to recognise and respond to the latest cyber threats.

Incident response

Incident response is the process that businesses use to manage and address cybersecurity alerts as they happen. It focuses on quickly identifying, managing, and mitigating incidents to minimise damage and prevent future occurrences. This process is a necessary part of rapid action and containment, ensuring that you can minimise the potential damage from real cybersecurity incidents. Incident responders play a crucial role in this, distinguishing genuine security threats from false alarms and providing the necessary rapid action to contain these threats.

Are you here?

Many companies, especially small to medium-sized businesses (SMBs), lack dedicated incident responders or a formal process for handling cybersecurity alerts.

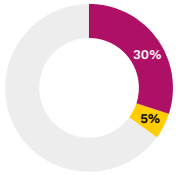


Our data shows that 44% of SMBs don't have a full incident response plan in place. Of the 18% without any plan at all, only 6% are planning to implement one in the next year.

This could lead to delayed or inadequate responses to real threats, as businesses might struggle to identify which alerts are genuine or critical. The absence of a structured incident response can expose businesses to significant risks, especially when sophisticated cyber-attacks occur.

Indeed, while some companies do have dedicated incident response teams, they aren't able to operate effectively, as they're often diverted from the real threats by having to deal with many false positives (or false alarms), which could distract, delay, or desensitise them to the warning signs.
Additionally, 24/7 monitoring is critical, as attackers often choose to strike outside business hours or on public holidays.

Best practice



30% of SMBs have a fully implemented incident response plan and keep it regularly updated, but we can see that 5% are still in the initial planning stages.

As businesses grow and evolve, the value of a dedicated incident response team or a security partner for incident response becomes clear. With dedicated professionals trained to quickly assess alerts, determine their validity, and take appropriate action to contain and mitigate threats, you can rest more easily, knowing that procedures are in place for rapid response.

In response to a widespread phishing campaign, a well-planned incident response might begin by initially blocking the senders and then moving to understand who may have been compromised, swiftly resetting access before any significant damage can occur. Similarly, in the case of a ransomware attack, a solid incident response would involve isolating affected systems to prevent further spread.

To illustrate how the modern threat landscape is speeding up, the Unit 42 Incident Response Report found a significant shift in attack vectors. In 2024, there has been a 39% increase in the exploitation of internet-facing vulnerabilities and 20.5% of breaches have begun with the use of compromised credentials as the initial access points.[iv]

Attackers are employing faster, more automated methods to compromise systems. To deal with this, SMBs need an agile incident response capability, either by developing internal capabilities or partnering with specialists to manage these cybersecurity threats effectively.

[iv] https://unit42.paloaltonetworks.com/unit42-incident-response-report-2024-threat-guide/

If you only do one thing...

Make it a priority to respond, investigate, and contain, where necessary, all incidents reported by your security tools. This means you're always prepared to take immediate action against potential cybersecurity threats, minimising the impact on your business operations.

Next steps

Explore options which will enhance your incident response capabilities, such as partnering with a service that specialises in managing security threats. This approach grants you access to the expertise of trained professionals and advanced tools and technologies, improving your ability to respond to incidents as soon as they happen.

54%

Given that only 54% of SMBs have a plan fully implemented, this is a great way to get your incident response plan off the ground quickly.

Also, focus on developing a comprehensive incident response plan. This plan should detail specific steps to take during different types of security incidents, designate roles and responsibilities within your team, and include procedures for post-incident analysis to learn from each event.

THE 6 KEY ELEMENTS OF INCIDENT RESPONSE

- **Prepare:** Make sure all staff understand their roles and the tools required are readily available.
- **Detect:** Implement systems to quickly identify security breaches.
- **Analyse:** Examine the incident in detail to understand its nature and scope.
- **Contain:** Taking immediate action to limit the spread or impact of the incident, protecting sensitive data and business operations.
- **Eradicate:** Remove the threat from the system entirely to prevent further damage or reoccurrence.
- **Recover:** Restore systems and operations to normal and learn from the incident to strengthen future response efforts.

Security awareness training

No matter the size of your company, every cybersecurity strategy you pull together needs to account for the behaviour of individuals . While technical controls play a key role, cybercriminals are increasingly focusing their efforts on exploiting an organisation's employees and third parties. Think of it this way: you could have the best home security system in the world, but if you open the front door and let in the bad actors, it won't make a difference. Helping your staff to recognise the warning signs is key if you want to tackle the causes, rather than the symptoms.

The potential business impacts from a successful phishing, social engineering or malware incident can be devastating - crippling operational downtime, theft of sensitive data, financial fraud, and reputation damage that erodes customer trust .

Security awareness training introduces a structured way to ensure all team members have the proper guidance to help them avoid falling victim to attacks. A well-trained team can act as a "human firewall," avoiding pitfalls like falling for phishing scams, clicking untrusted links, and succumbing to social engineering tactics that lead to invoice fraud, supplier impersonation, payment redirection, or identity theft. However, these threats are continually evolving, so to remain relevant, education needs to evolve alongside them.

Are you here?

It is not uncommon for businesses to leave their teams to fend for themselves, relying solely on common sense regarding suspicious communications. This means that team members have varying levels of healthy scepticism about dubious links, websites, or unsolicited messages, and no systemic approach to handling these instances.

In our research, 62% of SMBs employ online modules for security awareness training, which indicates a shift towards digital learning environments, but despite these efforts, 9% of organisations do not measure the effectiveness of their training at all, potentially missing insights into their training's impact.

In many SMBs, some guidance might be shared sporadically, but without regular reminders or inclusion of new employees. This results in uneven preparedness, with the most vulnerable individuals becoming easy targets for sophisticated threats with short memories when it comes to security awareness. Indeed, while 33% run regular knowledge assessments and quizzes to measure the effectiveness of security awareness training, only 23% of SMBs run cyberattack simulations and only 13% run industry benchmarking.

Best practice

Forward-thinking organisations understand that security awareness training is a non-negotiable pillar of their cyber defences. An educated workforce provides an essential last line of protection when technical controls fail or have gaps. These firms have recognised the importance of a more structured and measurable approach to security awareness with complete coverage across the team.

This training doesn't need to be difficult—it can be tailored to the specific threats the organisation is most concerned about. It's regular but concise, addressing people's tendency to forget over time but avoiding putting the blame on employees or using fear-based messaging.

Alex Bransome, *Chief Information Security Officer*
Doherty Associates

Security awareness training should be delivered in bite-size modules and integrated with existing HR training programs, including the new employee onboarding process.

The most effective training includes a practical element. For instance, coupling awareness training with regular simulated phishing tests can measure the training's effectiveness and identify individuals who need additional coaching.

In our research, the most common formats of security awareness training among SMBs are:

- **Online modules (62%)**
- **In-person sessions (e.g. workshops) (40%)**
- **Newsletters, updates, and PSAs (36%)**

Good security awareness training involves, among other things:

- A tailored curriculum for your organisation's top threat vectors, based on risk assessments and incident data.
- Mandatory training for all employees, contractors, and partners with access, refreshed at least annually.
- Engaging, interactive content using microlearning, gamification, scenarios, and storytelling.
- Frequent simulated phishing tests with reporting to reinforce training through experience.
- Integration with compliance training, reducing fatigue through unified risk awareness.
- Continuous content updates aligned to evolving threats, tailored by role and threat intelligence.

If you only do one thing...

Regularly remind your team about the main threats, warning signs to look for, and the importance of maintaining a "question first" mindset. Simple reminders can reinforce their role as the last line of defence.

QUICK TIP:

If you keep track of incidents caused by lack of security savviness – phishing breaches, improper data handling, policy violations, and so on – this helps you understand where these reminders will have the most impact.

For example, are your employees most susceptible to falling for phishing scams? Do they struggle with identifying suspicious attachments in emails? Are there frequent incidents of sensitive data being left unsecured on personal laptops?"

Next steps

Adopt a structured security awareness tool or managed service to make training a routine part of your cyber defences. Couple awareness initiatives with simulated phishing tests to validate training effectiveness and identify team members requiring more guidance.

You can also integrate security awareness with other employee training like HR policies, anti-bribery, and anti-money laundering for a streamlined experience.

Identity security

Identity security is all about controlling who can access different parts of your IT systems and ensuring they are who they say they are. As businesses increasingly move to cloud-based services, managing access has become the top priority to prevent unauthorised entry.

Identity security involves practices like user authentication, managing user permissions, and monitoring access activities. Effective identity security protects against identity-based attacks, which are becoming more common with the rise of sophisticated phishing and social engineering campaigns.

Are you here?

Businesses may rely on simple password-based systems to control access. This can be risky as passwords are often weak, reused across different services, or can be easily stolen through phishing attacks.

5%

Our research highlights that there has been growing awareness about the importance of layered identity security, as now only 5% of SMBs have no identity security measures in place.

A common issue faced by businesses is a breach due to compromised credentials, where attackers gain access through stolen or guessed passwords. With a compromised account, hackers might engage in activities like internal or external payment fraud, extracting sensitive data, or even sending phishing emails from a trusted internal account, leading to widespread compromise within the organisation.

EXAMPLE

Identity security failures were central to the effectiveness of the MGM Resorts cyberattack that crippled operations across its properties in early 2023. The incident began when a criminal hacking group known as Scattered Spider used stolen credentials and social engineering to breach MGM's network.

Through a vishing (voice phishing) attack, the threat actors tricked an employee into resetting their multi-factor authentication, gaining initial access. This ransomware attack had a cascading impact, disabling systems controlling hotel door locks, reservations, point-of-sale terminals and even slot machines across MGM's casino resorts like Bellagio and MGM Grand.

This breach emphasises the need for stronger privileged access safeguards, multi-factor authentication processes, monitoring of identity provider configuration changes, and rigorous security for critical tier 0 assets like identity management systems.

Best practice

The more mature approach involves, at minimum, implementing stronger security measures like Multi-Factor Authentication (MFA). **Our research showed that 76% of SMBs use MFA, but only 22% used biometric verification (e.g. fingerprint or facial recognition) and only 21% used passwordless authentication. While the latter two, more advanced options are less commonly used, they can enhance security by adding layers that are hard for attackers to fake.**
With more workers working from home, or coming in and out of the office, monitoring for risk signals, such as suspicious sign-in attempts from unusual locations, has become very important—as have the appropriate tools for alerting on this. If you want to prevent further unauthorised access, malicious sign-ins need to be identified quickly, along with immediate actions like resetting affected users' passwords.

In recent years, regulatory bodies like NIST and the Cybersecurity and Infrastructure Security Agency (CISA) have issued new guidelines emphasising the importance of passwordless authentication and continuous identity verification to combat modern threats. The NIST Digital Identity Guidelines were updated in 2022 to emphasise the need for more secure, phish-resistant authentication methods like passwordless and biometric solutions.[v]

Meanwhile, in 2023, (CISA) and the National Security Agency (NSA) released new guidance titled Identity and Access Management: Developer and Vendor Challenges to advocate for a 'zero trust' approach: continuously verifying user and device trust rather than relying only on initial login credentials.[vi]

Identity Access Management (IAM) solutions are critical security controls which can provide stronger security measures. This is an area experiencing rapid progression: many security controls make life harder for users, but enabling biometrics and passwordless authentication increases security and makes life easier for users. In fact, users often thank you for implementing these security measures!

While technical controls and advanced authentication are crucial, identity security ultimately comes down to the human element. All your employees and users are a critical part of the defence, not just IT or security staff, so ensuring they understand and engage with identity security Best practices is just as important as the technology itself.

If you only do one thing...

Implement MFA across your IT systems. This simple step adds a significant layer of security beyond just passwords. It's also crucial to enforce MFA for all accounts via a policy to ensure it stays enabled for all existing and any new accounts when they're created. This policy is quickly becoming the minimum bar for identity security.

Next steps

Consider exploring advanced IAM solutions – like biometric verification or passwordless authentication. Regularly monitor for and respond to risk signals such as unusual login attempts. Quick action in these situations, like resetting passwords, can prevent major security incidents. Also, where possible, stay informed about the latest trends in IAM and continually update your strategies to include phish-resistant MFA and other emerging technologies.

Finally, ensure you have dedicated personnel, or partner with a 3rd party trained in identifying and mitigating compromised identities.

[v] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf
[vi] https://media.defense.gov/2023/Oct/04/2003313510/-1/-1/0/ESF%20CTR%20IAM%20MFA%20SSO%20CHALLENGES.PDF

Endpoint detection and response (EDR)

Endpoint detection and response (EDR) is a cybersecurity step-change for SMBs. EDR goes far beyond traditional antivirus by actively monitoring endpoints—laptops, desktops, servers, and so on—for suspicious activities, in addition to known threats like viruses and malware. With its ability to run behavioural analysis on files and applications on each device, EDR spots anomalies, automatically intervenes, and even reverses malicious actions, allowing it to act as a vigilant watchdog for your digital estate.

Are you here?

Many businesses still rely on traditional antivirus software, believing this alone will give them sufficient protection. Traditional antivirus works on a react-and-respond model, chasing after known threats using a known pattern. These patterns then must be updated multiple times per day just to keep the antivirus software capable of recognising new threats.

When you're dealing with unknown threats, however, the game gets more complicated. Our research shows that at least 7% of SMBs do not use EDR solutions, which may leave them vulnerable to undetected endpoint threats. After all, you don't know what you don't know. Over the years, viruses and malware have evolved to evade this pattern-scanning behaviour, which effectively renders traditional antivirus software useless. Even when it does see the threat, it has a limited number of weapons in its arsenal: quarantining or deleting files. It also isn't able to create the kind of audit trail that you need to carry out a comprehensive review or fix the problem itself. With antivirus alone, organisations lack the necessary protection against modern threats like credential theft, identity compromise and privileged access abuse that antivirus is ill-equipped to handle.

Best practice

EDR does more than improve on traditional antivirus. It replaces it entirely. The old pattern-based system to recognise known threats gives way to a behaviour-based approach. EDR looks at all software and files – how they're behaving and interacting – to find threats, which means it doesn't have to rely on you having seen this type of threat before.

EDR scrutinises every action on your network, looking for anything out of the ordinary. By keeping a detailed audit trail, EDR not only spots but also learns from each incident, offering insights into how a breach occurred and how to prevent it in the future. The moment your EDR classes an application as malicious, you can go into that audit trail to understand exactly what's happened and speed up your remediation process dramatically. For example, if EDR detects ransomware activity on a device, you'd be able to understand what files and websites were accessed and which settings were changed.

Perhaps one of EDR's most notable features is its ability to automatically undo the chaos an attacker might leave behind. From deleting malicious files to reversing configuration changes, EDR can often restore order without manual intervention. Also, if an endpoint is compromised, EDR can isolate it, preventing the spread of malware to other parts of your network. Not only does this cut back on the human effort required, it also means you can respond faster and more effectively to active threats.

Like any team, your cybersecurity tools perform best when they work together. EDR's strength lies in its ability to integrate with other security tools, sharing intelligence across the board. 20% of firms we surveyed integrate EDR with their other security tools, which enhances their defence and gives a bird's eye view of their digital estate: for example, has anyone clicked this malicious link? Has another networked laptop downloaded that file? EDR helps you get the answers you need faster, and, most importantly, it doesn't wait for you to tell it to get started.

Caleb Mills
Professional Services Director
Doherty Associates

"Imagine you download a PDF and open it in Adobe Reader, but instead of the document, a command prompt (a programme that allows direct entry of commands in Windows) launches unexpectedly.

"This is where EDR comes in: immediately detecting this anomalous activity and taking action to prevent the command prompt from fully launching or executing any malicious commands. Once detected, the EDR solution can terminate the suspicious process, isolate the affected endpoint, and provide detailed reporting and forensics to aid investigation and remediation."

Of the 309 SMB leaders we spoke to, the top ways they were using their EDR solutions were:

- **Detecting suspicious activity (57%)**
- **Preventing malware and ransomware (52%)**
- **Real-time monitoring (36%)**

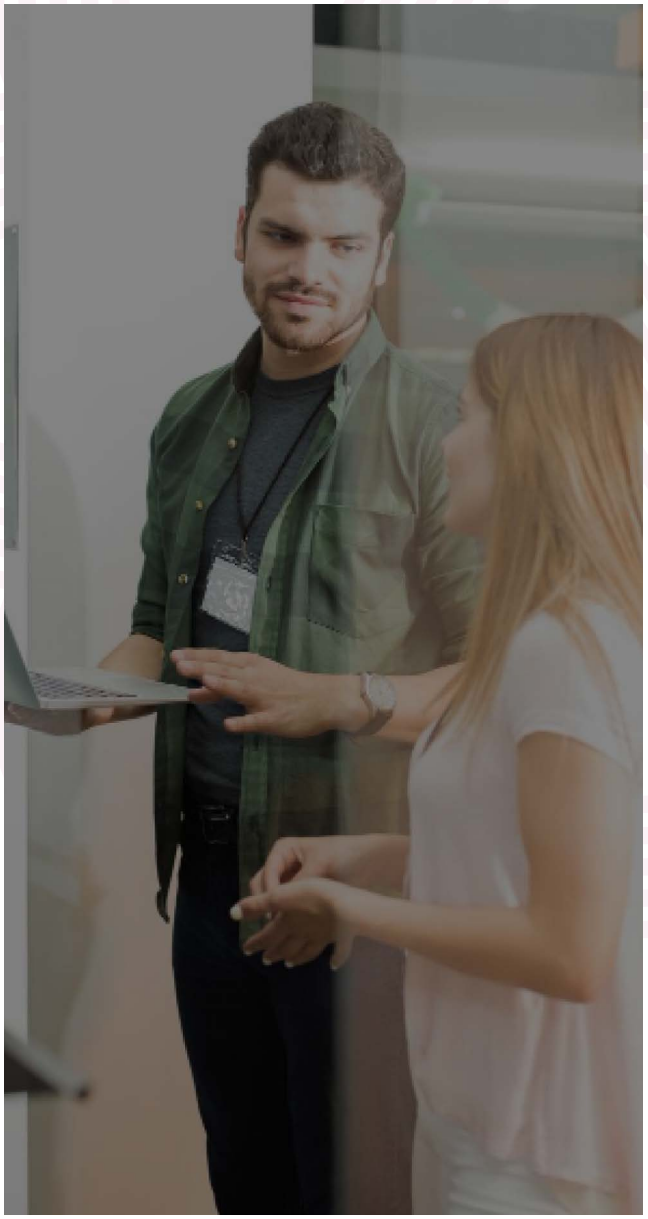
If you do one thing...

Uninstall your antivirus and replace it with EDR. No matter how good it is at pattern-based detection, your antivirus is no longer fit for purpose. By focusing on the behaviour of threats, rather than their signatures, EDR will give you a more dynamic and proactive defence against the increasingly sophisticated cyberattacks that traditional antivirus may miss.

Next steps

Start by allowing your EDR system the autonomy to isolate or remediate threats as they are detected. This step can significantly speed up your response time, as it eliminates delays caused by human decision-making processes. It also ensures that any potential breach can be contained with greater efficiency. Also, don't forget to integrate your EDR system with the rest of your security infrastructure.

It's essential that every team member knows their role and that there is a clear protocol for addressing security concerns across various devices, from laptops to servers. For some organisations, it may be prudent to consider a partnership with a Managed Detection and Response provider. This not only brings in external expertise but also ensures that threat detection and response are always in capable hands.



Cloud access security broker (CASB)

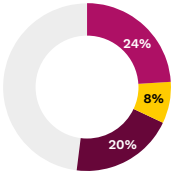
Despite the cloud revolutionising how businesses operate, offering unparalleled flexibility, scalability, and cost savings, it's also introduced new security risks. The shift to cloud-based services has introduced potential vulnerabilities that traditional on-premises solutions may struggle to address. Here's where the Cloud Access Security Broker (CASB), a critical cybersecurity tool for businesses embracing the cloud, comes in.

Think of a CASB as a security checkpoint for all your cloud traffic. It scans and monitors the access and activities within your cloud applications, keeping an eye on traffic and ensuring that only the right people can get in and sensitive data doesn't leak out. CASBs are particularly valuable for SMB leaders who may not have the in-house expertise to fully secure their cloud environments. A CASB can extend your traditional on-premises security measures to the cloud, giving you the control and oversight you need to protect your data and operations.

Are you here?

Many businesses still underestimate the unique security challenges posed by cloud computing. The focus is often on reaping the benefits of cloud services - like flexibility and cost savings - without fully grasping the need for specialised cloud security measures.

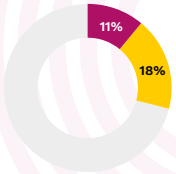
This oversight could lead to serious incidents. For example, inadequate access controls in a cloud setting can lead to unauthorised data access. In traditional IT, physical and network perimeters often protect data, but in the cloud, data can be accessed from anywhere, which means that robust user authentication and strict access policies are crucial. Without visibility, monitoring, and control of their cloud environment, many firms risk data breaches and compliance issues that can severely damage their reputation and bottom line.



Despite the clear benefits, our findings show that 24% of SMBs do not use a CASB, while 8% have evaluated but not yet implemented a CASB solution. Additionally, a notable 20% of businesses are unfamiliar with CASB, suggesting a significant opportunity for education and adoption in the sector.

Best practice

As businesses have become more aware of the security implications of cloud computing, the adoption of CASB solutions has grown commensurately. We're seeing many companies who now recognise the importance of having a dedicated security layer that specifically addresses the risks inherent in cloud environments.



11% of SMBs are implementing these systems extensively for multiple cloud applications, while 18% keep them in place for critical applications only.

Caleb Mills, *Chief Technology Officer*
Doherty Associates

"The cloud has blurred the traditional security perimeter, so businesses need a way to stitch together visibility and control across all their digital assets. An integrated CASB is the glue that binds these disparate security solutions into a cohesive, defence-in-depth strategy."

POPULAR CASB TOOLS

Looking for a CASB tool that fits your organisation's needs? Here are some of the most popular solutions:

- **Microsoft Defender for Cloud Apps:** Providing visibility, risk assessment, and access control for cloud apps, especially for those using Microsoft 365 and Azure.
- **Cisco Cloud Security (Cloudlock):** Focused on protecting data, detecting threats, and enforcing DLP policies across cloud services.
- **Symantec CloudSOC CASB:** Offering data security, user behaviour analytics, and compliance management for cloud applications.

To see which one works best for you, why not chat with other IT leaders and see which one they recommend? Alternatively, you may want to consider having a consultation with a qualified Managed Security Services Provider to gain a professional perspective.

CASBs can also uncover 'shadow IT' - the unsanctioned cloud applications that employees might be using without your knowledge. By shining a light on this hidden attack surface, you can take steps to mitigate the risks associated with these rogue services.

By integrating a CASB into your cybersecurity strategy, you gain the visibility and control needed to confidently embrace the cloud while keeping your data and operations secure.

It's worth noting, however, while a CASB is a powerful tool for cloud security, it works best when integrated with other security solutions, such as SIEM, EDR, and identity management systems.

For more information, see our sections on SIEM, EDR, and Identity Security.

However, the most successful organisations know that implementing a CASB is not a "set-it-and-forget-it" solution. To maintain its effectiveness, the CASB configuration and rulesets must be regularly reviewed and optimised. As new cloud applications are adopted, user behaviours change, and threats evolve, the CASB policies need to be refined to ensure they accurately reflect the company's risk tolerance and security requirements.

If you only do one thing...

Start by conducting an inventory of your cloud applications and evaluating your current cloud security measures. Understanding what cloud services you use and how they're protected is the first step towards identifying the need for a CASB solution.

Next steps

Consider deploying a CASB to gain greater visibility and control over your cloud environment. Look for solutions that align with your business's specific cloud usage patterns, security requirements, and compliance obligations.

Develop a comprehensive cloud security strategy that includes CASB, regular security assessments, shadow IT discovery, and employee training on cloud security Best practices. By implementing a CASB and incorporating it into a broader cloud security plan, you'll be able to reap the benefits of cloud computing while effectively managing the associated risks.

Security information and event management (SIEM)

Security information and event management (SIEM) acts as a central nervous system for your organisation's digital defences. SIEM solutions collect and analyse log data from various sources within your IT infrastructure, such as servers, network devices, and applications. By looking for patterns and signs of potential security threats, like unauthorised access attempts or suspicious activities, SIEM helps identify and respond to complex cybersecurity incidents.

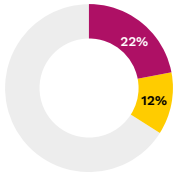
In simpler terms, think of SIEM as a unified security control centre. It gathers all the security alerts from across your digital environment, analyses them to determine if there's a genuine threat, and then alerts your security team. For example, a SIEM for 100 people might ingest 20 million events in a month, generate 20 events for a human to investigate, and of those 20 events, 5 might be real cyber threats or incidents. This allows your analysts to quickly respond to issues, sometimes even before any real damage is done.

SIEM not only helps in identifying and responding to threats but also retains logs for a duration of time, enabling threat hunting where suspicious activities can be investigated in detail after the fact. Additionally, incorporating SOAR (Security Orchestration, Automation, and Response) capabilities can automate responses based on detected signals, enhancing the efficiency and effectiveness of your security operations.

While SIEM solutions are powerful tools, they require investment and resources to implement and maintain effectively. Smaller businesses with more limited IT environments may want to initially explore more lightweight security monitoring and log analysis options.

Are you here?

Businesses often manage security through disparate tools, each monitoring a different aspect of IT security.



Indeed, 22% of businesses we surveyed did not have any type of SIEM tool in use. 12% of respondents, however, responded that they did use a SIEM, but it operated independently of other IT management tools.

This fragmented approach often leads to critical alerts being missed or not acted upon in time, as there's no central system to correlate the information between systems.

Best practice

In a more advanced setting, SIEM comes into play, integrating data from across the business's IT environment. It helps in quickly identifying and correlating unusual patterns that could indicate a security breach. A SIEM solution not only alerts the team about potential threats but also assists in response and investigation, providing a consolidated view of security data.

16%

16% of organisations we surveyed have achieved full integration of SIEM with their IT and security management tools, enhancing real-time threat detection and response capabilities across their digital environments.

Indeed, regulatory requirements today, such as GDPR, often mandate extensive logging and security monitoring capabilities – SIEM solutions can help to address this requirement. Similarly, the shift to remote and hybrid work models has significantly increased the attack surface for many organisations. With employees accessing corporate resources from a variety of locations and devices, comprehensive monitoring and visibility across the entire environment has become even more critical.

SCENARIO

Imagine a sophisticated spear-phishing attack targeted at your organisation. The attacker, having done preliminary research, sends a crafted email to several employees. The email appears to come from a trusted source, perhaps mimicking a common communication style seen within the company.

The SIEM system continuously receives and analyses data from the email security system, the identity provider, and audit logs and correlates these disparate pieces of information. It recognises the pattern—an email containing a suspicious link, followed by unusual login activity and peculiar user behaviour. The SIEM system alerts the cybersecurity team with this correlated information, highlighting the potential spear-phishing attack.

Armed with specific, correlated information from the SIEM system, the cybersecurity team can quickly investigate the incident. They can trace the origin of the attack, identify affected systems, and reset the compromised credentials. They can use this incident's data to strengthen their defences against similar future attacks.

In this scenario, the SIEM system acts as a central hub, connecting signals from various sources that might seem unrelated at first glance. By doing so, it enables the cybersecurity team to detect, analyse, and respond to complex threats in a more informed and timely manner.

If you only do one thing...

If you're just starting out with SIEM, make sure you're ingesting the right logs into your system. Carefully select logs that are most relevant to your security needs, such as logs from critical systems, sensitive data repositories, and key network devices. This focused approach not only ensures that you're monitoring the most crucial data but also helps manage costs associated with SIEM log ingestion.

Next steps

Training your team or partnering with a service provider for effective SIEM management is vital, as the system's effectiveness largely depends on the skills of the people operating it. Next, define your log retention period and dedicate resources to fine-tuning your SIEM's alert system. This involves adjusting the system to reduce false positives and ensure that the alerts you receive are meaningful and actionable.

Customised dashboards within your SIEM solution can give you real-time insights into your security posture, helping you quickly understand your current threat landscape and make informed decisions. Finally, based on that assessment and your organisation's changing needs, review and update your SIEM configurations and rulesets regularly.

Cyber insurance

Cyber insurance acts as a safety net for your business. It was designed to help companies deal with the financial fallout from cyber threats like hacking, data breaches, and other online risks. This type of insurance can cover a range of costs, including those for investigating what went wrong, fixing security holes, legal fees if you're sued, and even public relations efforts to repair your reputation.

While cyber insurance does cover a range of costs and liabilities, common exclusions to watch out for include court jurisdictions (e.g. North America is often excluded from policies bought in the UK), bodily injury or property damage, or losses as a result of damage to critical national infrastructure (CNI), among others.

As cyber threats become more common and sophisticated, having cyber insurance is becoming an essential part of a business's defence strategy—not just for recovery, but also for gaining access to specialised support when you need it most. Cyber insurance can provide a crucial fallback, helping you bounce back quickly from an incident and minimising the long-term damage to your operations and reputation.

Are you here?

In the early days of digital-focused businesses, cyber insurance was often a novel and overlooked tool – though that has changed significantly in recent years. Many companies operated under the assumption that their existing security measures are sufficient, or simply accept the risk of cyber incidents as an unavoidable cost of doing business.

This mindset, however, leads to businesses being unprepared for the financial and reputational damage from cyberattacks. For example, without cyber insurance, we might see a small firm suffering a data breach, leading to costly legal battles, regulatory fines, and lost customer trust without any financial safety net. Indeed, third-party research shows 75% of SMBs could not continue operating if they were hit with ransomware.[vii]

23%

A surprising 23% of firms we surveyed remain without any form of cyber insurance, potentially exposing them to severe financial risks following cyber incidents.

After a cyber breach, the cost of data recovery can be prohibitive, especially for SMBs. A study by IBM found that the average cost of a data breach in 2023 was $4.45 million, up 16% in three years, a significant portion of which is attributable to data recovery.[viii]

Best practice

Today, there's a growing recognition of the importance of cyber insurance as part of a holistic cyber security strategy. Of the SMBs we surveyed, the top aspects of risk covered by their cyber insurance policy were data breaches (48%), ransomware attacks (40%), and legal fees and fines (34%), demonstrating a maturation in risk management strategies. Businesses now understand that no defence is perfect and that the impact of cyber incidents can be significantly mitigated with the right insurance coverage.

To see how this evolution has taken shape, imagine a company that experiences a ransomware attack but is able to recover quickly with minimal financial impact, thanks to its cyber insurance policy. This policy not only covers the ransom payment but also provides expert assistance in navigating the crisis, showcasing the multifaceted value of cyber insurance.

Parametric cyber insurance policies are quickly gaining popularity because they provide faster payouts and reduce the burden of proving loss. Unlike traditional indemnity policies, parametric covers pre-defined events (e.g. ransomware infection, DDoS attack – even downtime for cloud, eCommerce, or payment services) and automatically triggers payments, allowing organisations to rapidly access funds for response and recovery.

[vii] https://www.strongdm.com/blog/small-business-cyber-security-statistics#small-business-cyber security-overview:~:text=75%25%20of%20SMBs%20could%20not%20continue%20operating%20if%20they%20were%20hit%20with%20ransomware.%C2%A0

[viii] https://www.ibm.com/reports/data-breach

COMMON CYBER THREATS COVERED BY CYBER INSURANCE:

- Malware/viruses
- Hacking
- Cyber crime
- Data breaches
- DDoS attacks
- Cyber extortion
- Network outages
- Business interruption
- Data loss/corruption
- Crisis management
- Incident response
- Notification costs
- Security audits
- Privacy violations
- Regulatory defense
- Cyber ransom payments

When considering the addition of business interruption losses to your cyber insurance policy, it is crucial to understand that the financial impact of downtime extends far beyond immediate revenue loss. This type of insurance can provide compensation for the loss of income during periods when your company's operations are halted due to cyber incidents, helping to stabilize cash flow and maintain business continuity.

If you only do one thing...

Review your current cybersecurity measures and assess the potential financial impact of a cyber incident on your business. For instance, what would be the potential cost if a cyberattack resulted in the theft of sensitive client data, incorporating the expenses associated with legal fees, increased security measures, lost sales, and customer compensation?

This will help you understand the importance and need for cyber insurance in your specific context. Knowing the potential costs and risks your business faces can give you the proof you need to prioritise cyber insurance at an organisational level and secure buy-in from budget stakeholders.

Next steps

Consider consulting with a cyber insurance specialist to explore coverage options that align with your business's specific risks and needs. Tailoring your policy to cover the most relevant threats can provide both financial and operational peace of mind.

Additionally, implement regular reviews of your cyber insurance coverage as part of your overall cybersecurity strategy. As your business grows and evolves, so too will your exposure to cyber threats, which adds to the need for periodic adjustments to your insurance coverage to make sure it remains adequate.

Business continuity/Disaster recovery

When we talk about Business continuity and Disaster recovery (BC/DR) in cybersecurity, we're referring to the processes and procedures that make sure a company can continue to operate and quickly recover in the event of a cyberattack or data breach. BC/DR is your emergency plan, preparing you and ensuring that your business operations can withstand and quickly rebound from cyber incidents.

It's important to understand the difference between Business continuity and Disaster recovery. BC focuses on quickly recovering after an incident, often by failing over to redundant systems. DR, on the other hand, involves the process of recovering everything from backup, which takes significantly longer than a failover to redundant systems.

For SMBs, integrating BC/DR into your cybersecurity strategy is critical. Even a short period of downtime can lead to significant financial losses and erode customer trust. Implementing a robust BC/DR plan means you're not only able to respond to cyber threats but also recover quickly, minimising the impact on your business operations and reputation.

Are you here?

For many businesses, BC/DR planning has, at best, only been broadly sketched out. Plans often go untested, leaving companies unsure of their effectiveness. Backup processes exist, but without regular monitoring, their reliability is questionable. In addition, the scope of these plans is limited, focusing mainly on servers and databases, neglecting critical components like email systems and employee access to digital resources.

Terry Doherty, *Founder and Chief Executive*
Doherty Associates

"The key to effective business continuity planning is to think beyond just data backups. It's about having a holistic strategy that ensures all critical functions, from communications to supply chain, can continue with minimal disruption. Regular testing is crucial - you need to know your plan works before you have to put it into action."

BEAR IN MIND

The General Data Protection Regulation (GDPR) requires that personal data breaches are reported within 72 hours of becoming aware of the breach, necessitating robust incident response plans as part of BC/DR strategies.

This narrow approach can leave businesses vulnerable, as untested recovery plans and unmonitored backups could fail when most needed. For instance, a company might discover too late that their backups were corrupted, rendering them useless in the aftermath of a cyberattack. Another scenario could involve having functioning backups and even conducting some restores, but if the entire system is unavailable, do you have all the passwords and documentation needed to facilitate a full restore from backup?

In addressing the challenges associated with testing BC/DR plans, our findings reveal that 40% of organisations cite a lack of resources, such as time or funding, as a primary obstacle. In addition, 34% struggle with insufficient technical expertise within their teams, which complicates the simulation of realistic scenarios essential for effective testing. Most concerning is that 10% of businesses do not have a formalised BC/DR plan, potentially leaving them unprepared for cyber incidents that could disrupt operations significantly.

Best practice

A strong BC/DR plan doesn't just include data backups; it also contains comprehensive plans that detail how to maintain operations during and after a cyber incident.

Modern BC/DR strategies emphasise comprehensive scope and regular testing. Today, disaster recovery plans include all critical systems and data, ensuring that operations can be restored fully, not just partially. Regular testing of disaster recovery plans and backup recovery processes has become a norm, enabling businesses to identify and rectify issues before they impact recovery efforts.

By implementing a comprehensive BC/DR plan and staying proactive in your approach, you're laying a strong foundation to weather even the most severe cyber storms. When disaster strikes, you'll have the confidence that your business can continue operating and bounce back quickly, minimising the impact on your customers, reputation, and bottom line.

CASE STUDY

'In June 2022, Macmillan Publishers, one of the largest book publishers in the U.S., fell victim to a significant cyberattack, likely ransomware, that forced it to shut down its IT systems. The attack resulted in the encryption of certain files on its network. As a precautionary measure, Macmillan immediately took systems offline, closed its virtual and physical offices in New York, and faced disruptions in its ability to process and ship book orders.

In response, Macmillan worked with specialists to investigate the incident, restore functionality, and implement additional network safeguards. By June 28th, its UK warehouse resumed operations, and it began bringing certain systems back online. The company demonstrated transparency by communicating updates to customers, partners, and employees throughout the recovery process.'

If you only do one thing...

Ensure you have a detailed Disaster Recovery (DR) plan for your business and commit to testing it regularly. This is the single most crucial step you can take to protect your business from the fallout of a cyber incident.

Next steps

Develop a more sophisticated threat intelligence strategy and conduct periodic backup restoration tests to verify the integrity and effectiveness of your backups. This means you can rely on them when you need them most.

Run a thorough risk assessment to prioritise and protect your most critical assets – making sure your BC/DR strategies are aligned with your business's specific needs and vulnerabilities.

Review and update your BC/DR plan regularly. This may involve incorporating lessons learned from testing, addressing new vulnerabilities, or adjusting recovery time objectives as your organisation changes.

How Doherty Associates can help

Cyber-attacks are growing increasingly sophisticated, and choosing the right security partner is crucial to keeping your business safe. Many in-house security teams are over-stretched or lacking in essential skills, and many incumbent security partners are providing insufficient protection, support and value for money.

Doherty Associates creates, maintains, and develops IT systems that are secure by design.

Cyber security roadmap

We craft tailored strategies and actionable steps to future-proof your business wherever you are on the cyber curve.

Over-stretched IT teams

We alleviate IT burdens with cyber experts operating as an extension of your team, freeing you to focus on core tasks.

Hybrid working risks

We help you unlock productivity and collaboration to ensure seamless and secure working for your remote workforce.

Compliance & regulatory challenges

We help you navigate complex regulations and avoid penalties and legal issues.

Phishing prevention

We turn your employees into a 'human firewall', educating them to detect phishing attempts and malicious attacks.

Cyber security accreditation assurance

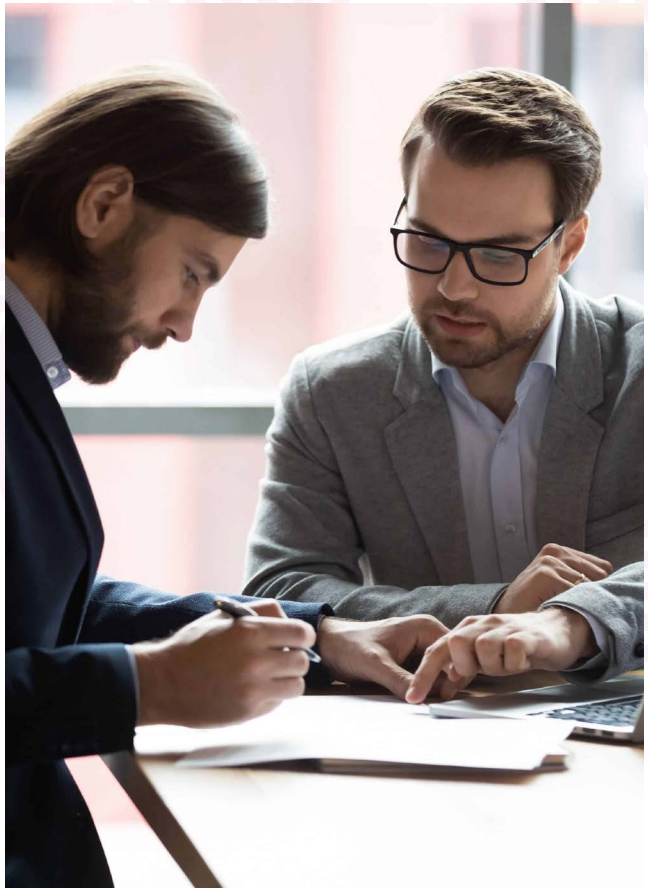
We guide you through the accreditation processes to provide internal and external reassurance through these standards.

Security in the cloud

We facilitate secure migration to the cloud – from platform selection to unlocking benefits and cost efficiencies.

Demystifying cyber security jargon

We simplify complex terms and enhance understanding, empowering you to make informed decisions.



However fledgling or well-developed your IT security posture, we're confident we can add value to it, so please contact us if you think we can help.

Our cyber security services

Strategic security leadership

Strategic guidance from our experienced team, from cyber security governance, to compliance, risk and response management, and data protection. Enabling points of weakness to be addressed and ensuring your organisation meets its legal and regulatory obligations.

Managed detection and response (MDR)

Identifying, analysing, and neutralising cyber threats in real-time, our MDR service provides proactive measures to safeguard your sensitive data and maintain operational integrity in the face of evolving and ever more sophisticated threats. Our threat protection covers devices, identities, apps, email, data and cloud workloads.

Security operations centre (SOC)

Leveraging a robust Security Information and Event Management (SIEM) system and industry-leading defence and orchestration tools to detect sophisticated cyber threats often missed by more traditional technologies. A proactive response to cyber threats at speed and preventing future occurrence.

Security assessments

Our security assessments offer a holistic approach to evaluating and fortifying your organisation's security posture. Through meticulous analysis and strategic recommendations, we help you identify vulnerabilities, mitigate risks, and achieve compliance with industry standards and regulations. Partnering with Doherty Associates provides you with a strategic security roadmap, in-depth security insights, bespoke risk profiling, cutting-edge threat intelligence, and rigorous control evaluation.

Cyber security insights

Our expert team, with deep industry knowledge and experience, focuses on stripping out the noise to help you concentrate on the data and alerts that truly matter. By effectively analysing your security data, we provide tailored recommendations to enhance your cyber defence strategy, ensuring you are equipped to tackle the most significant threats to your organisation.

Security awareness training & phishing simulation

Comprehensive training and phishing simulation to empower your employees with the knowledge and skills needed to recognise and respond to cyber threats effectively. We help to turn your workforce into a 'human firewall' by ensuring they understand the potential impact of phishing and other social engineering techniques, along with how they can help to keep your organisation safe.

About Doherty Associates

Doherty Associates is a London-headquartered IT consultancy and service provider with over 30 years of experience providing technology solutions and 24/7 managed services for our clients, including banks, venture capital and private equity firms, and fund and asset managers.

Nominated as Best Managed Services Provider at the private fund operations focussed Drawdown awards, in 2021 (winners) and 2023, Doherty Associates understands the pressures and expectations of working with financial services organisations. With a client attrition of just 1.4% in 2022, service excellence singles out Doherty Associates in a services market that is both crowded and diverse.

Terry Doherty, *Founder and Chief Executive*
Doherty Associates

Here at Doherty Associates, we can help you chart your position on the spectrum compared with the higher performing organisations in your sector. We call this process Smartpath, where we help you to think about your existing IT operating model vs good practice and common industry standards, to land your best IT strategy and action plan.
That's our offer to you.

Microsoft partnership

As a longstanding Microsoft partner, Doherty Associates has satisfied the rigorous requirements of experience, customer satisfaction and know how to be recognised as being in the top tier of Microsoft's 'partner ecosystem'. Our five main Microsoft Solutions Partner designations span the crucial areas of security, cloud computing, data analysis, communication and collaboration, and server infrastructure.

Microsoft Solutions Partner
Modern Work

Microsoft Solutions Partner
Infrastructure
Azure

Microsoft Solutions Partner
Digital & App Innovation
Azure

Microsoft Solutions Partner
Data & AI
Azure

Microsoft Solutions Partner
Security