TECHN22

Techn22 Threat Report 2024

Exploiting Weak Defences and Targeting Critical SME Data

Ransomware remains the most common Cyber Threat facing UK SMEs in 2024.

National Cyber Security Centre (NCSC)

Contents

The Rising Cyber Threat Landscape for SMEs

Small and medium-sized enterprises (SMEs) in the UK face a significantly heightened risk in the cybersecurity landscape. Once considered less likely targets, SMEs are increasingly in the crosshairs of cybercriminals. Cyberattacks against SMEs have become more frequent, sophisticated, and destructive, making cybersecurity a crucial business priority.

The misconception that SMEs don't possess valuable data is fading fast. These businesses often have access to sensitive client information, financial records, and intellectual property, making them lucrative targets for cybercriminals.

In 2023, the National Cyber Security Centre (NCSC) reported a dramatic increase in cyberattacks on UK SMEs, with **39%** of small businesses confirming at least one cyber breach during the year.

This statistic highlights a critical issue: SMEs are often less equipped to defend against cyberattacks, lacking the resources of their larger counterparts. As a result, the consequences of a cyberattack—such as financial loss, operational disruption, and reputational damage—can be far more devastating for an SME.

The Evolution of Cybercrime: Why SMEs are Targeted

Cybercriminals have evolved their tactics and strategies, making it increasingly clear that no business is too small to be targeted. Many SMEs believe that cyberattacks are primarily aimed at larger organisations with vast amounts of sensitive data. However, cybercriminals are opportunistic. SMEs are often seen as "soft targets" because they typically invest less in cybersecurity and may not have the resources to recover quickly from a breach.

The growing adoption of cloud computing, remote work, and the use of third-party vendors has expanded the attack surface for SMEs. These technological shifts, while increasing efficiency, have also introduced new vulnerabilities that cybercriminals exploit. Many SMEs fail to realise that a single successful cyberattack could be devastating—research from the Cyber Security Breaches Survey 2023 found that **60%** of SMEs that suffer a major cyberattack go out of business within **six months**.

Common Cybersecurity Challenges Faced by SMEs

- **Limited Budgets for Cybersecurity:** Unlike larger corporations, SMEs often operate on tight budgets, which limits their ability to invest in robust cybersecurity tools and infrastructure. Cybercriminals are well aware of this and specifically target businesses that lack sophisticated defences.

- **Lack of Cybersecurity Expertise:** SMEs typically lack dedicated cybersecurity staff, leaving their IT teams stretched thin. This lack of expertise makes it easier for cybercriminals to exploit security weaknesses that would likely be addressed in larger organisations.

The Rising Cyber Threat Landscape for SMEs

- **Outdated Technology:** Many SMEs continue to rely on outdated hardware and software that are no longer supported by vendors. These unpatched systems leave businesses vulnerable to known exploits and attacks. In fact, the NCSC warns that unpatched systems are one of the leading causes of breaches in the UK.

- **Human Error:** Human error is a significant contributing factor in most cyberattacks. Employees in SMEs may not have access to regular cybersecurity training, making them more susceptible to phishing emails, weak passwords, and accidental data leaks.

The Financial and Reputational Impact of a Cyberattack

For SMEs, a cyberattack can be far more than an IT inconvenience—it can be an existential threat. The financial toll of a cyberattack can include costs associated with data recovery, system downtime, and legal fees, not to mention potential fines for failing to meet GDPR or other regulatory requirements.

A 2022 report by IBM estimated the average cost of a data breach for an SME to be **£1.6 million**. This figure includes the direct costs of dealing with the breach and the long-term effects, such as reputational damage and loss of business. For an SME, these costs can be unsustainable.

In addition to financial losses, a cyberattack can severely damage a business's reputation. Clients and customers expect their data to be protected, and a data breach can erode trust that took years to build. This is particularly critical for SMEs that operate in industries with sensitive data, such as healthcare, financial services, or legal firms.

The Growing Threat Landscape: Key Cybersecurity Trends Impacting SMEs

The cybersecurity threat landscape is rapidly changing, and SMEs need to stay vigilant. Some of the most pressing trends include:

- **Ransomware Attacks:** Ransomware remains one of the most common and damaging threats to SMEs. In 2023 alone, ransomware attacks against UK businesses increased by 45%, with SMEs accounting for a significant portion of the targets. Ransomware-as-a-Service (RaaS) models have made it easier than ever for criminals to launch attacks, even with minimal technical skills.

- **Phishing Scams:** Phishing remains the top vector for cyberattacks against SMEs. Phishing attacks, where cybercriminals trick employees into clicking malicious links or providing sensitive information, accounted for **83% of breaches in UK SMEs** last year, according to the Cyber Security Breaches Survey. The sophistication of these scams has increased, with attackers using social engineering tactics to personalise their attacks, making them harder to detect.

- **Supply Chain Attacks:** SMEs are also vulnerable to supply chain attacks, where cybercriminals target the weakest link in the supply chain to gain access to larger, more lucrative businesses. The NCSC has warned that supply chain attacks are on the rise, with **62% of SMEs reporting being impacted by an attack** through a third-party vendor.

The Rising Cyber Threat Landscape for SMEs

Why SMEs Must Prioritise Cybersecurity Now

As the cyber threat landscape continues to change, SMEs cannot afford to be complacent. The cost of failing to invest in cybersecurity can be catastrophic. However, implementing cybersecurity measures doesn't have to be expensive. Government-backed programs, such as Cyber Essentials, provide SMEs with affordable solutions to protect themselves from common cyber threats.

SMEs must adopt a proactive cybersecurity strategy that includes:

- **Employee training and awareness:** Educating staff on how to recognise phishing emails and use strong passwords is essential.

- **Regular software updates:** Keeping systems and software up-to-date can prevent attackers from exploiting known vulnerabilities.

- **Dark web monitoring:** SMEs can reduce the risk of compromised data by monitoring the dark web for signs that sensitive information is being traded.

By taking these proactive steps, SMEs can significantly reduce their risk of falling victim to cyberattacks, safeguarding both their financial health and reputation.

Conclusion

Cybercrime is no longer a distant concern for large corporations; it's an imminent threat for SMEs in the UK.

The combination of limited resources, outdated technology, and increasing sophistication of cybercriminals means that SMEs must take immediate action to protect themselves.

Prioritising cybersecurity is no longer optional—it's a fundamental business need that can determine the long-term survival and success of an SME.

Top Cybersecurity Threats in 2024

The cyber threat landscape for SMEs changes constantly, with new forms of attacks emerging and existing threats becoming more sophisticated.

In 2024, several key threats continue to dominate the cybersecurity landscape, putting small and medium-sized businesses at significant risk.

This section will highlight the most prevalent threats SMEs need to be aware of, including ransomware, phishing, insider threats, and AI-driven attacks.

Ransomware: The Most Devastating Threat

Ransomware attacks remain the most significant and damaging threat to SMEs in 2024.

Ransomware is a type of malicious software that encrypts a business's data, making it inaccessible until a ransom is paid. This type of attack can completely paralyse a business, shutting down operations and putting critical data at risk.

The National Cyber Security Centre (NCSC) has reported a **45% increase** in ransomware attacks on UK businesses in 2023, and this trend is expected to continue through 2024 and beyond. What makes ransomware particularly devastating is the rise of Ransomware-as-a-Service (RaaS), which allows even novice cybercriminals to execute sophisticated attacks. RaaS operates on a subscription-based model, where experienced cybercriminals create ransomware kits and lease them to other criminals. This has lowered the barrier to entry for ransomware attacks and led to a proliferation of incidents.

In 2024, ransomware attacks have also evolved with a new tactic known as double extortion. In these cases, cybercriminals not only encrypt a company's data but also threaten to release sensitive information unless the ransom is paid. This puts SMEs in an even more difficult position—pay the ransom to regain access to data or face the risk of sensitive information being leaked.

45%

increase in ransomware attacks on UK business in 2023

National Cyber Security Centre (NCSC)

Top Cybersecurity Threats in 2024

Key Statistics:

- **51%** of businesses experienced a ransomware attack in 2023.
- The average ransom demand in 2023 was **£170,000**, while the overall cost of a ransomware attack (including downtime and recovery) can **exceed £3 million**.
- **62%** of SMEs targeted by ransomware end up paying the ransom, though 1 in 3 businesses that pay still do not recover all their data.

SMEs can protect themselves from ransomware by implementing robust backup and disaster recovery solutions. Regular backups ensure that businesses can restore their data without paying a ransom.

Additionally, businesses should invest in security awareness training for employees to recognise phishing emails, which are often the initial entry point for ransomware attacks.

Phishing Attacks: The Gateway to Cybercrime

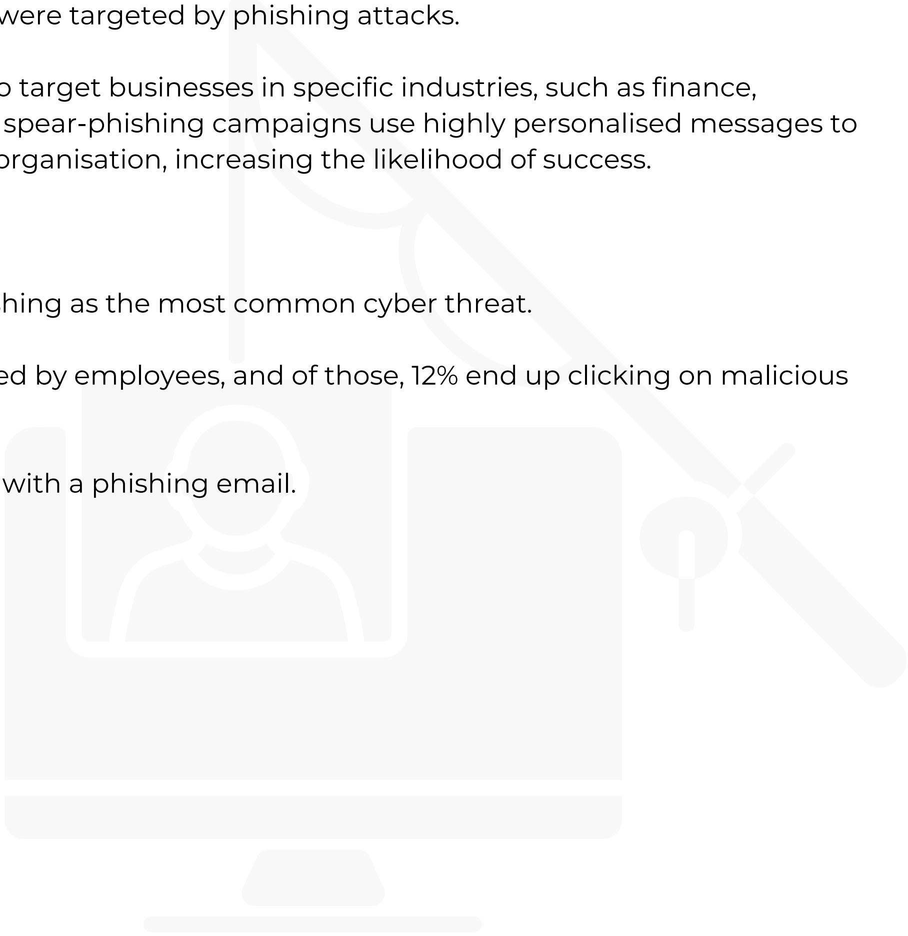
Phishing attacks continue to be the most common form of cyberattack on SMEs. Phishing involves cybercriminals sending deceptive emails that trick employees into revealing sensitive information or downloading malicious software. The sophistication of phishing emails has increased significantly, with attackers using more personalised approaches to deceive employees.

Phishing is not only a standalone threat but also a gateway to more severe attacks like ransomware and credential theft. According to the Cyber Security Breaches Survey 2023, **83%** of UK businesses that experienced a cybersecurity breach were targeted by phishing attacks.

Phishing attacks have also evolved to target businesses in specific industries, such as finance, healthcare, and legal services. These spear-phishing campaigns use highly personalised messages to target specific individuals within an organisation, increasing the likelihood of success.

Key Statistics:

- **83%** of UK businesses report phishing as the most common cyber threat.
- **30%** of phishing emails are opened by employees, and of those, 12% end up clicking on malicious links.
- **95%** of ransomware attacks start with a phishing email.



Top Cybersecurity Threats in 2024

Insider Threats: A Hidden Danger

Insider threats—whether from malicious employees or accidental actions—are a growing concern for SMEs. As businesses adopt hybrid and remote work models, managing employee access to critical systems has become more complex. This increases the risk of insiders, either knowingly or unknowingly, exposing the business to cyber risks.

Malicious insiders may intentionally steal data or compromise systems for financial gain, while negligent insiders may fall victim to social engineering attacks, resulting in unintentional data leaks. According to the NCSC, insider threats account for **34%** of cyber incidents in the UK.

Key Statistics:

- Insider threats account for **34%** of data breaches in the UK.
- **70%** of insider incidents are caused by employee negligence rather than malicious intent.

To mitigate insider threats, SMEs should enforce strict access controls that limit who can view and modify sensitive data. Regular audits of employee access and permissions are crucial to preventing unauthorised access to critical systems.

Additionally, businesses should deploy monitoring tools that detect unusual user behavior, flagging any suspicious activity before it results in a breach.

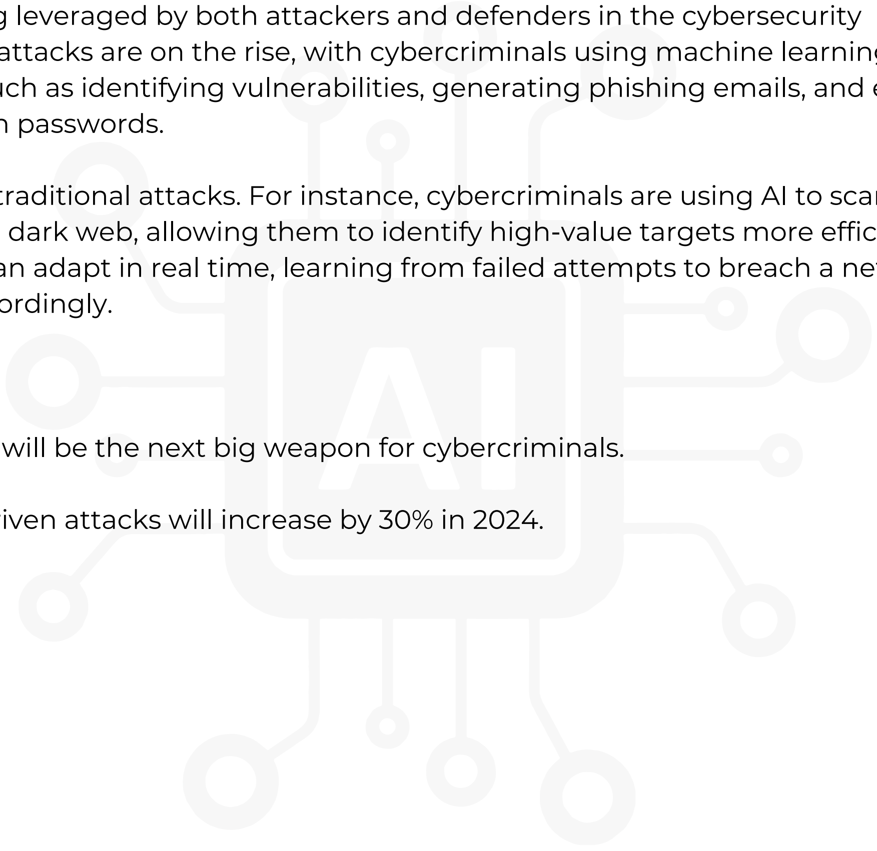
AI-Driven Cyber Attacks: A New Era of Threats

Artificial intelligence (AI) is being leveraged by both attackers and defenders in the cybersecurity landscape. In 2024, AI-powered attacks are on the rise, with cybercriminals using machine learning algorithms to automate tasks such as identifying vulnerabilities, generating phishing emails, and even executing brute-force attacks on passwords.

AI can also be used to enhance traditional attacks. For instance, cybercriminals are using AI to scan massive amounts of data on the dark web, allowing them to identify high-value targets more efficiently. Additionally, AI-driven attacks can adapt in real time, learning from failed attempts to breach a network and refining their strategies accordingly.

Key Statistics:

- 60% of businesses believe AI will be the next big weapon for cybercriminals.
- The NCSC predicts that AI-driven attacks will increase by 30% in 2024.



Top Cybersecurity Threats in 2024

SMEs can defend against AI-driven attacks by implementing AI-powered cybersecurity solutions themselves. These solutions can detect anomalies and respond to threats in real time, helping businesses stay one step ahead of cybercriminals. Investing in behavioral analysis tools can also help identify suspicious patterns of behavior that indicate an impending attack.

Conclusion

The cybersecurity threat landscape for SMEs in 2024 is more dangerous and complex than ever. From the threat of ransomware to the rise of AI-driven attacks, SMEs must stay vigilant and invest in comprehensive security measures to protect their assets.

Understanding these top threats—and taking proactive steps to mitigate them—is essential for ensuring business continuity in an increasingly hostile digital environment.

Supply Chain Attacks

Increasing reliance on third-party vendors and partners has opened a new frontier for cybercriminals. In a world where businesses are connected through supply chains, a vulnerability in one link can expose an entire network.

Supply chain attacks are becoming a growing concern for SMEs, particularly as businesses increasingly adopt cloud services, SaaS platforms, and external contractors to streamline operations.

Moving forward, protecting these supply chains is critical for securing your business.

What is a Supply Chain Attack?

A supply chain attack occurs when cybercriminals exploit weaknesses in a third-party vendor or service provider to gain access to the primary target, which can be any business in the vendor's client base. Instead of attacking a business directly, attackers look for vulnerabilities in the interconnected systems of suppliers, contractors, and partners, which might be less secure. The goal is to infiltrate one link in the chain and pivot towards the main target, often an SME that may have sensitive data or valuable resources.

Cybercriminals often target the weakest link, which may be smaller, less resourced vendors. Once they gain access, they can use that entry point to move laterally through a company's systems and eventually target larger companies in the chain or the company itself.

Example: The 2020 SolarWinds attack, where attackers compromised the software updates of a trusted IT vendor, led to the infiltration of thousands of companies and government organisations. While this incident affected large corporations, SMEs in the supply chain were also compromised, illustrating how vulnerable smaller businesses are to supply chain breaches.

The Increasing Focus on Supply Chain Vulnerabilities

With more businesses adopting cloud solutions, external service providers, and integrated supply chain technologies, the attack surface has expanded significantly. According to the National Cyber Security Centre (NCSC), 62% of supply chain attacks in 2023 targeted SMEs, as they are often seen as the weakest link in a larger network. SMEs frequently partner with larger enterprises and other SMEs to share resources, access tools, and optimize operations.

This web of connections provides more entry points for attackers looking to exploit weak security measures.

62%

of supply chain attacks in 2023 targeted SMEs

National Cyber Security Centre (NCSC)

Supply Chain Attacks

Key Statistics:

- 60% of SMEs that suffered a cyberattack in 2023 were affected by supply chain vulnerabilities.
- 43% of businesses in the UK are now more concerned about supply chain cyber risks than they were a year ago.

Why SMEs are Particularly Vulnerable to Supply Chain Attacks

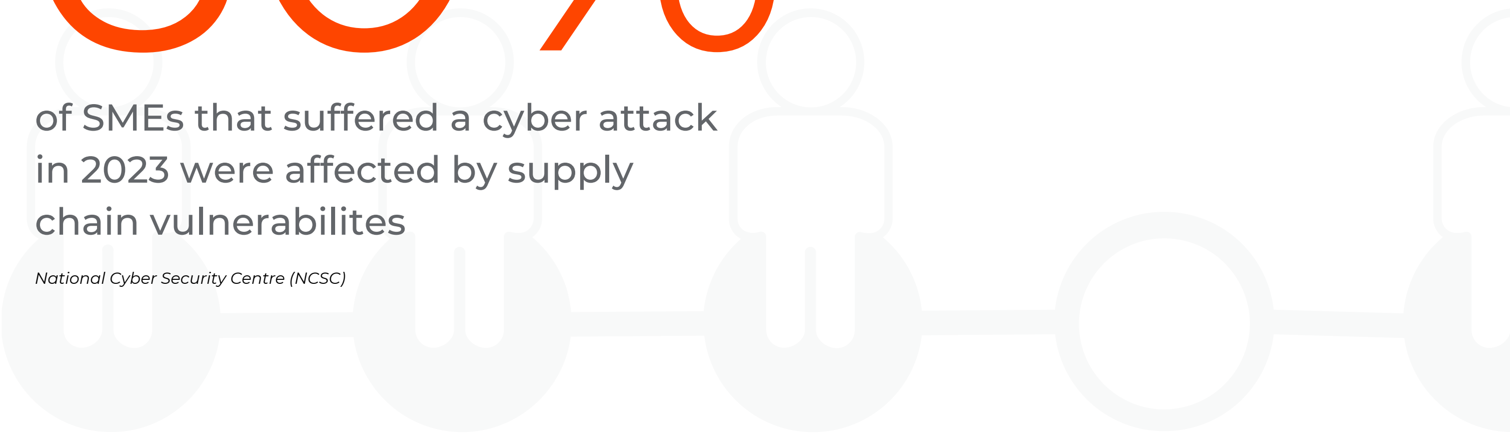
There are several reasons why SMEs are more vulnerable to supply chain attacks:

- **Lack of Comprehensive Vetting:** SMEs may not have the resources or expertise to thoroughly vet their third-party vendors' security practices. As a result, they may unknowingly partner with vendors who have inadequate cybersecurity measures in place.
- **Shared Systems:** Many SMEs share cloud-based systems and SaaS platforms with their vendors. If the vendor is compromised, the SME can also be at risk.
- **Understaffed IT Departments:** Smaller businesses often have limited or no in-house cybersecurity teams, making it harder to identify and respond to supply chain threats. This gives attackers an advantage, as they can breach systems with minimal resistance.
- **Interconnected Ecosystem:** As more SMEs adopt digital transformation technologies, they become increasingly interconnected with suppliers, customers, and service providers. This ecosystem is only as strong as its weakest link.

60%

of SMEs that suffered a cyber attack in 2023 were affected by supply chain vulnerabilites

National Cyber Security Centre (NCSC)



Supply Chain Attacks

How Supply Chain Attacks Affect SMEs

Supply chain attacks are particularly dangerous because they are difficult to detect. Many businesses may not realise they have been compromised until significant damage has been done. An attack on a supply chain can lead to:

- **Data Breaches:** A successful supply chain attack can result in unauthorised access to sensitive customer or business data, leading to severe financial and reputational damage.

- **Operational Disruption:** If a key supplier is attacked, it can disrupt the entire supply chain, causing production delays, logistical bottlenecks, and financial losses.

- **Financial Penalties:** Breaches caused by supply chain attacks can result in regulatory fines for non-compliance with data protection laws, such as the GDPR. Even if the attack originates with a vendor, the business may still be held responsible for failing to ensure adequate data protection.

Proactive Measures for Securing Supply Chains

While supply chain attacks are complex, there are steps that SMEs can take to mitigate these risks:

- **Due Diligence on Vendors:** Before entering into a partnership with a vendor, SMEs should conduct a thorough security assessment to ensure that the vendor follows best practices for cybersecurity. This includes ensuring that the vendor complies with industry regulations such as Cyber Essentials or ISO 27001.

- **Contractual Security Requirements:** Businesses should require vendors to meet specific cybersecurity standards as part of their contractual agreements. This can include stipulations for regular security audits, penetration testing, and incident response procedures.

43%

of businesses in the UK are now more concerned about supply chain cyber risks than they were a year ago.

National Cyber Security Centre (NCSC)

Supply Chain Attacks

- **Multi-Factor Authentication (MFA):** SMEs should enforce MFA not only for their internal systems but also for any third-party access to their data and networks. This prevents attackers from exploiting weak authentication protocols in the supply chain.

- **Continuous Monitoring:** Implement monitoring tools that provide real-time visibility into the security posture of your supply chain partners. These tools can help detect unusual activity or data breaches in real time, allowing businesses to respond quickly before significant damage is done.

- **Zero Trust Architecture:** Adopt a Zero Trust approach to security. This means that no entity, whether internal or external, is automatically trusted. All access requests are verified, and permissions are granted based on the principle of least privilege.

The Role of Cyber Insurance

Given the complexity of supply chain attacks, many SMEs are turning to cyber insurance to mitigate the financial risks. Cyber insurance policies can cover the costs associated with data breaches, business interruption, and regulatory fines. However, it’s important to note that cyber insurance alone is not a substitute for strong cybersecurity practices. SMEs must still prioritise risk management and proactive security measures.

Conclusion

Supply chain attacks represent a growing and serious risk for SMEs. With the increasing digital interconnectivity between businesses, a single vulnerability in a third-party provider can compromise an entire organisation. SMEs must be proactive in securing their supply chains by conducting due diligence on vendors, enforcing strong access controls, and adopting continuous monitoring tools.

By understanding the risks and taking appropriate action, SMEs can protect themselves from becoming the weakest link in their supply chain.

Emerging Threat - AI and Machine Learning in Cybersecurity

As artificial intelligence (AI) and machine learning (ML) technologies become more integrated into business processes, they present both opportunities and new cybersecurity challenges.

While AI helps automate cybersecurity defences and improves threat detection, it is also being used by cybercriminals to launch more sophisticated and harder-to-detect attacks. For small and medium-sized enterprises (SMEs), understanding the dual nature of AI is crucial to bolstering their cybersecurity defences.

How AI is Transforming Cybersecurity

AI and ML have brought a range of innovations to the field of cybersecurity. These technologies are capable of analysing vast amounts of data to detect anomalies, predict potential threats, and automate defensive responses. For example, AI-driven security tools can identify patterns of unusual behavior that might indicate a cyberattack, helping businesses detect and mitigate threats before they cause damage.

AI's ability to handle repetitive, large-scale data tasks makes it ideal for:

- **Threat Detection:** AI-based tools can continuously monitor networks, identifying threats in real time without human intervention. These systems can detect subtle anomalies that traditional tools may miss.

- **Predictive Analytics:** Using historical data, AI can predict potential security incidents before they happen. This enables businesses to adopt a proactive rather than reactive approach to cybersecurity.

- **Automation of Responses:** AI-driven systems can automatically block malicious activity or isolate compromised systems, allowing businesses to respond to threats faster and more efficiently.

While these advancements are promising, they come with new risks. Just as businesses are using AI to bolster their defences, cybercriminals are leveraging AI and ML to create more dangerous and effective attack strategies.

AI-Driven Cyberattacks: A Growing Threat

Cybercriminals have begun using AI to automate various stages of an attack, from identifying potential vulnerabilities to launching sophisticated phishing campaigns. AI's capacity for automation and learning enables attackers to operate at unprecedented speed and scale, targeting multiple businesses simultaneously.

Some key ways AI is being used by cybercriminals include:

- **Automated Phishing Attacks:** AI can be used to generate highly personalised phishing emails by analysing publicly available data from social media profiles, corporate websites, and other sources. This increases the chances of phishing emails being opened and acted upon by unsuspecting employees.

Emerging Threat - AI and Machine Learning in Cybersecurity

- **Malware Evolution:** AI-powered malware can adapt and evolve in response to security measures, making it harder to detect and eradicate. These programs can modify their code to avoid detection by traditional antivirus software, leaving businesses vulnerable.

- **Deepfake Attacks:** AI can generate highly convincing fake videos or audio clips (deepfakes), which can be used for social engineering attacks. For instance, deepfake technology has been used to impersonate business executives and trick employees into transferring large sums of money to cybercriminals.

Key Statistics:

- 60% of businesses expect AI-powered attacks to increase in 2024, according to a report from the NCSC.

- AI-generated phishing emails are three times more likely to succeed than traditional phishing attempts.

Balancing the Benefits and Risks of AI

While the rise of AI-driven cyberattacks poses new challenges for SMEs, AI remains a powerful tool for bolstering cybersecurity defences. Businesses that embrace AI for threat detection, analysis, and response can gain a significant advantage in the battle against cybercriminals. However, it's essential to approach AI implementation with caution, ensuring that the systems in place are continually updated and monitored to stay ahead of potential attackers.

Key Considerations for SMEs:

- **Adopt AI-Driven Cybersecurity Tools:** Invest in AI-powered cybersecurity tools that can detect threats in real-time and provide automated responses to minimise the damage of an attack.

- **Continuous Learning:** Ensure that your AI-based systems are regularly updated with the latest threat intelligence to keep up with evolving cyber threats.

- **Employee Training:** AI cannot completely replace human oversight. It's crucial to combine AI tools with ongoing employee training to ensure that staff can recognise potential threats and respond appropriately.

The Role of AI in Data Privacy and Compliance

AI also plays a critical role in helping businesses meet compliance requirements for data privacy laws such as GDPR. AI-driven tools can monitor for unauthorised access to sensitive data and flag any potential breaches before they escalate. Additionally, these tools can help businesses implement Zero Trust architectures, ensuring that employees and third parties only have access to the specific data and systems they need to perform their tasks.

Emerging Threat - AI and Machine Learning in Cybersecurity

Key Points:

- **Automated Compliance Monitoring: AI can monitor data access in real-time, ensuring that compliance requirements are met without overburdening human resources.**
- **Anomaly Detection: AI can flag unusual patterns of behavior in how data is accessed, helping businesses catch potential breaches early.**

AI in Cybersecurity: Moving Forward

For SMEs, AI is both a threat and an opportunity. The same technology that is being used to automate attacks can also be leveraged to create stronger, more resilient defences. It's essential that businesses strike a balance between utilising AI to bolster their cybersecurity posture while staying vigilant to the emerging risks posed by AI-powered threats.

Key Takeaways:

- AI-driven cyberattacks are on the rise, but businesses can leverage the same technology to improve their defences.
- SMEs should invest in AI-based cybersecurity tools while ensuring that they stay updated on the latest threat intelligence.
- Combining AI technology with ongoing employee training and a Zero Trust approach will help SMEs maintain a strong security posture in the face of AI-driven threats.

Conclusion

As AI continues to evolve, its role in both cybersecurity and cybercrime will grow. For SMEs, adopting AI-powered tools is no longer optional—it's a necessity for staying ahead of increasingly sophisticated threats.

However, it's equally important to remain aware of how AI can be used against your business, and to develop a robust, proactive cybersecurity strategy that leverages AI's strengths while mitigating its risks.

60%

60% of businesses expect AI-powered attacks to increase in 2024

National Cyber Security Centre (NCSC)

Cyber Resilience and Recovery Planning

Cyber resilience is not just about preventing cyberattacks but also about ensuring that businesses can recover swiftly when incidents do occur. For small and medium-sized enterprises (SMEs), cyber resilience encompasses preparation, defense, and the ability to maintain critical operations even when under attack. Recovery planning, on the other hand, ensures that businesses can quickly restore normalcy, minimise financial loss, and protect their reputation after a breach.

What is Cyber Resilience?

Cyber resilience refers to a business's ability to prepare for, respond to, and recover from cyberattacks while maintaining business continuity. It goes beyond traditional cybersecurity, which primarily focuses on preventing attacks, by emphasising the importance of minimising operational disruptions during an attack and accelerating the recovery process after an incident.

Given the sophistication of modern cyber threats, even the best-protected businesses can experience breaches. The key is not just preventing these attacks but having robust systems in place to reduce downtime and recover as quickly as possible. For SMEs, this is especially critical since 59% of SMEs report that a successful cyberattack leads to significant downtime, and 40% of these businesses never fully recover.

Key Statistics:

- 70% of UK SMEs admit they are not fully prepared to respond to a cyberattack, according to the NCSC.

- 93% of organisations that suffered a breach in 2023 reported operational disruption lasting more than a week.

Importance of a Cyber Resilience Strategy

A cyber resilience strategy is essential for SMEs because cyberattacks are inevitable. While preventative measures like firewalls and antivirus software reduce the likelihood of attacks, they cannot guarantee full protection. The importance of a cyber resilience strategy lies in its ability to help businesses respond swiftly and maintain business continuity in the face of disruption.

A good cyber resilience strategy should include:

- **Proactive Defense Measures:** Strong prevention tactics such as employee training, multi-factor authentication (MFA), and regular system updates.

70%

of UK SMEs admit they are not fully prepared to respond to a cyberattack

National Cyber Security Centre (NCSC)

Cyber Resilience and Recovery Planning

- **Incident Response Plan:** A clear and detailed action plan outlining the steps that need to be taken immediately after a cyberattack, including who is responsible for handling communications, containment, and recovery.

- **Backup and Recovery Solutions:** Regularly backing up critical data ensures that a business can restore operations quickly, without being forced to pay a ransom or suffer extended downtime.

Case Study:

A UK-based SME suffered a ransomware attack in 2023, which encrypted all their client data. However, because they had a robust recovery plan and data backup strategy in place, they were able to restore their systems within 48 hours without paying the ransom. This illustrates the power of cyber resilience planning.

Key Components of a Strong Recovery Plan

Once a cyberattack has occurred, the immediate priority for any business is to restore normal operations with minimal disruption. A comprehensive cyber recovery plan focuses on both the technical aspects of recovery and the communication strategy, helping SMEs regain trust and credibility with stakeholders.

Some key elements include:

- **Data Backup and Restoration:** Ensuring that critical business data is backed up regularly and can be restored quickly. SMEs should employ a combination of on-premises and cloud-based backups to ensure redundancy.

- **Business Continuity Planning:** A business continuity plan (BCP) outlines the essential services and processes that need to continue running, even during a cyber incident. This might include alternative methods of customer communication, working remotely, or ensuring product deliveries continue as planned.

- **Communication Protocols:** After a breach, it's essential to communicate promptly and transparently with clients, customers, and stakeholders. Having a predefined communication plan ensures that the business can provide accurate updates and manage reputation damage effectively.

93%

of organisations that suffered a breach in 2023 reported operational disruption lasting more than a week

National Cyber Security Centre (NCSC)

Cyber Resilience and Recovery Planning

Key Statistics:

- 92% of businesses that have a cyber resilience plan in place report that they were able to recover from incidents within three days, compared to 56% of businesses without a formal plan.

Recovery Beyond the Technical: Reputation and Compliance

Beyond restoring systems and data, SMEs need to think about recovering their reputation. A successful breach can lead to a loss of trust from clients, which can be far more damaging than the technical impact of the attack. SMEs need to show that they take security seriously, and having a cyber resilience plan in place is part of that demonstration.

Additionally, compliance with data protection regulations such as GDPR is critical. SMEs must be prepared to respond to regulatory authorities following a breach and show that they had systems in place to protect customer data. Failure to comply can result in heavy fines and further reputational damage.

The Role of Techn22 in Building Cyber Resilience

At Techn22, we understand the unique challenges SMEs face when it comes to building cyber resilience. Our team works closely with businesses to develop tailored resilience strategies that focus on prevention, detection, and recovery. Whether it's implementing proactive solutions like multi-factor authentication and dark web monitoring, or providing comprehensive recovery plans and regular system backups, we ensure that SMEs are fully equipped to handle cyber incidents.

Conclusion

Cyber resilience and recovery planning are no longer optional—they are essential for businesses to survive. By adopting a proactive approach, SMEs can minimise downtime, protect their data, and maintain customer trust, even in the face of increasingly sophisticated cyberattacks.

Solutions for SMEs

Cybersecurity is critical for small and medium-sized enterprises (SMEs) as they increasingly face cyber threats that can have serious financial and operational consequences. While large corporations often have extensive resources dedicated to cybersecurity, SMEs can adopt practical, cost-effective solutions to protect themselves. This section focuses on key cybersecurity measures SMEs can implement to safeguard their operations.

Cyber Essentials Certification: Building a Security Foundation

One of the most effective steps for SMEs to bolster their cybersecurity is achieving Cyber Essentials certification. Cyber Essentials is a government-backed certification scheme from the National Cyber Security Centre (NCSC) that provides SMEs with the essential cybersecurity controls needed to protect against the most common threats. These controls ensure that businesses have the basic protection necessary to defend against attacks such as malware, ransomware, and phishing.

Cyber Essentials helps SMEs implement five key controls:

- **Firewalls:** Ensures that all internet connections to and from the business are secure.
- **Secure Configuration:** Ensures that all devices and systems are set up correctly and securely.
- **Access Control:** Only authorised individuals can access data and systems.
- **Malware Protection:** Safeguards against malware infections through anti-virus and other defences.
- **Patch Management:** Ensures that software is updated regularly to patch known vulnerabilities.

Cyber Essentials certification is a solid baseline for businesses to demonstrate their commitment to cybersecurity. It provides peace of mind to customers and clients while ensuring businesses are protected from common attacks. Additionally, many organisations now require Cyber Essentials as a prerequisite for doing business, making it a vital credential for SMEs.

Solutions for SMEs

Key Statistics:

- 75% of SMEs that adopt Cyber Essentials report reduced vulnerability to cyberattacks.
- The Cyber Security Breaches Survey 2023 found that 43% of businesses experienced cybersecurity incidents related to inadequate basic controls.

Dark Web Monitoring: Proactively Protecting Business Data

The dark web is an unregulated part of the internet where stolen data, including passwords, financial records, and confidential business information, is often traded. SMEs, in particular, are vulnerable to the consequences of sensitive data being exposed on the dark web. Dark web monitoring is a proactive service that scans for compromised business credentials and alerts companies if their information is detected on illicit forums.

For SMEs, dark web monitoring provides a critical early warning system. By identifying compromised credentials before they are used maliciously, businesses can take action to reset passwords, strengthen defences, and prevent unauthorised access. This is especially important for companies that store sensitive customer data or proprietary information.

Phishing Simulation and Cyber Training: Strengthening the Human Firewall

Phishing attacks are one of the most common forms of cyberattacks, and they rely heavily on human error. SMEs are particularly vulnerable to phishing, where employees are tricked into clicking malicious links or providing sensitive information through fraudulent emails. Training employees to recognise phishing attempts is one of the most effective ways to prevent these attacks.

Regular phishing simulations help educate employees by exposing them to real-world scenarios in a controlled environment. Over time, this practice reduces the likelihood of falling for phishing scams and strengthens the overall security posture of the organisation.

Cybersecurity training should also focus on other key areas, including password hygiene, multi-factor authentication (MFA), and secure communication practices.

Key Statistics:

- 95% of cybersecurity breaches are attributed to human error.
- SMEs that conduct regular phishing simulations experience 40% fewer successful phishing attacks than those that don't.

95%

of cybersecurity breaches are attributed to human error

National Cyber Security Centre (NCSC)

Solutions for SMEs

Penetration Testing: Identifying Vulnerabilities Before Cybercriminals Do

Penetration testing, also known as pen testing, involves simulated cyberattacks conducted by ethical hackers to identify vulnerabilities in a business's network and systems. These controlled attacks help businesses uncover security weaknesses before malicious hackers can exploit them.

For SMEs, penetration testing provides a clear picture of where improvements are needed to prevent unauthorised access and breaches. These tests are especially important for identifying weak spots in systems handling sensitive data or those required to comply with industry regulations.

At Techn22, we offer CREST-accredited penetration testing that adheres to industry standards and provides comprehensive security assessments. For many SMEs, the cost of penetration testing can be a concern.

That’s why Techn22 provides affordable penetration testing services that can be spread over 12 months, making it easier for businesses to maintain regular assessments without stretching their budget.

Key Benefits:

- **Proactive Risk Identification:** Pinpoints vulnerabilities before they can be exploited by cybercriminals.
- **Improved Security Posture:** Provides actionable insights for strengthening systems.
- **Regulatory Compliance:** Helps businesses stay compliant with industry and government cybersecurity regulations.

Conclusion: Proactive Cybersecurity for SMEs

Cybersecurity is a critical concern for SMEs, and taking proactive steps to protect business assets, data, and systems is essential.

By adopting solutions like Cyber Essentials certification, dark web monitoring, phishing simulation and training, and penetration testing, SMEs can greatly reduce their exposure to cyber risks.

These measures not only protect businesses from the financial and operational impact of cyberattacks but also provide peace of mind and ensure compliance with industry standards.

Cyber Threat Case Study

One of the most impactful ways to understand the importance of cybersecurity is through real-world case studies.

These examples show how cyberattacks can affect businesses, their operations, finances, and reputations. For small and medium-sized enterprises (SMEs), learning from others' experiences can highlight both the dangers of neglecting cybersecurity and the benefits of being proactive in preventing attacks.

Case Study 1: Ransomware Attack on a UK SME

In 2023, a UK-based SME in the financial services sector fell victim to a ransomware attack. Despite having basic cybersecurity measures in place, they were targeted by a sophisticated ransomware group. The attackers infiltrated the company's network through a phishing email sent to an employee, which contained a malicious attachment. Once opened, the ransomware encrypted critical business files, rendering all operational data inaccessible.

The ransom demand was set at £150,000, with the attackers threatening to leak sensitive customer information if the company refused to pay. Due to the nature of the business, which relied heavily on client trust and data security, the breach posed significant reputational damage. The company had a limited cybersecurity budget and no specific plan to respond to such an attack, forcing them into negotiations with the attackers.

Consequences:

- The company experienced three weeks of downtime, severely affecting business operations and customer service.
- Despite paying the ransom, not all files were recovered, causing a permanent loss of data and increased operational costs to rebuild systems.
- The financial loss exceeded £300,000, which included the ransom, IT recovery costs, and reputational damage.

Lessons Learned:

- The SME could have prevented the attack by investing in phishing simulations and employee training to educate staff on how to recognise suspicious emails.
- A comprehensive backup strategy would have allowed the company to restore data without paying the ransom.
- Ransomware defence tools, such as multi-factor authentication (MFA) and real-time malware monitoring, could have detected the breach earlier and stopped the encryption process.

Cyber Threat Case Study

Case Study 2: Insider Threat in a Manufacturing SME

A mid-sized manufacturing company in the UK experienced a cyber breach caused by an insider threat. A disgruntled employee with access to sensitive company information intentionally leaked confidential data to a competitor. The employee had been overlooked during routine security checks and had access to data far beyond the scope of their role.

Over the course of several months, the employee slowly extracted intellectual property and financial documents, using cloud storage platforms to move data offsite. The breach was only discovered after the employee left the company, at which point significant damage had already been done.

Consequences:

- The company suffered a loss of intellectual property, leading to a competitive disadvantage in the market.
- Legal costs rose as the company pursued action against the former employee and sought damages for the stolen data.
- The incident caused internal trust issues within the company, affecting employee morale and leading to stricter internal data policies.

Lessons Learned:

- A Zero Trust security framework, where no user is automatically trusted, could have limited the insider's access to sensitive data.
- Regular access audits and a stronger access control policy could have restricted the employee’s ability to view or transfer sensitive information.
- Implementing data loss prevention (DLP) software would have flagged the unauthorised data transfers and mitigated the damage earlier.

Cyber Threat Case Study

Case Study 3: Supply Chain Attack on a Retail SME

A retail SME in the UK that relied on an external vendor for payment processing fell victim to a supply chain attack. The vendor's systems were compromised, allowing cybercriminals to access the SME's payment processing infrastructure. As a result, customer payment details were stolen and sold on the dark web, leading to widespread fraud cases among the company's clients.

Although the SME had invested in basic cybersecurity for its internal operations, the breach originated from the vendor's side, which was not adequately vetted for security compliance.

Consequences:

- The SME faced severe reputational damage as customers lost trust in the business's ability to protect their financial information.
- The business was forced to pay for credit monitoring services for affected customers and faced regulatory fines under GDPR for failing to adequately protect client data.
- Revenue losses mounted as customers switched to competitors following the breach.

Lessons Learned:

- Conducting due diligence on third-party vendors and ensuring they comply with cybersecurity standards could have prevented the attack.
- The SME should have implemented multi-factor authentication and end-to-end encryption for payment transactions to protect customer data.
- Regular vendor security assessments would have allowed the business to spot vulnerabilities in the supply chain before they could be exploited.

Conclusion: Learning from Real-World Incidents

These case studies demonstrate the severe consequences SMEs can face when cyber threats go unchecked. From financial loss to reputational damage and operational disruption, the impact of a cyberattack can be devastating. However, they also highlight key lessons on how these incidents could have been avoided with proactive security measures.

Investing in cyber resilience, such as dark web monitoring, phishing simulations, penetration testing, and employee training, can help SMEs reduce the risk of falling victim to similar attacks. Learning from these real-world examples can provide invaluable insights for businesses looking to strengthen their defences in today's increasingly dangerous cyber environment.

Conclusion - Moving Forward with Proactive Cybersecurity

As businesses, particularly SMEs, continue to operate in an increasingly digital world, cybersecurity must be seen as a crucial component of long-term success. The reality is that cyber threats are ever-present and evolving, making it imperative for companies to adopt a proactive, rather than reactive, approach to their digital security.

The Importance of Vigilance

The evolving threat landscape highlighted in this report underscores the need for constant vigilance. Cyberattacks no longer only target large corporations; small and medium-sized enterprises are increasingly at risk due to their perceived weaker defences. From ransomware to phishing attacks, and insider threats to AI-driven attacks, SMEs face a myriad of threats that could severely damage their financial health, reputation, and operations.

The case studies included in this report clearly show the consequences of failing to implement adequate cybersecurity measures. Whether it's a ransomware attack leading to financial loss or a supply chain breach causing reputational damage, these examples serve as a stark reminder that the costs of not being prepared can far outweigh the investment in proactive cybersecurity solutions.

Proactive Measures: The Key to Cyber Resilience

The most effective way for SMEs to combat these threats is by taking a proactive approach to cybersecurity. Rather than waiting for an attack to happen and dealing with the fallout, businesses should focus on prevention, detection, and resilience. Some of the key proactive measures discussed throughout this report include:

- **Achieving Cyber Essentials certification:** This government-backed certification provides businesses with a solid cybersecurity foundation, helping them protect against the most common cyber threats.

- **Dark Web Monitoring:** This service allows businesses to detect compromised data on the dark web before it can be exploited, giving them time to mitigate the damage.

- **Phishing Simulations and Employee Training:** Given that human error is a leading cause of cyber breaches, educating employees and conducting regular phishing tests can significantly reduce the risk of successful attacks.

- **Penetration Testing:** By identifying vulnerabilities before cybercriminals do, penetration testing provides businesses with the insights needed to strengthen their security defences.

- **Backup and Recovery Solutions:** Implementing a robust backup and recovery plan ensures that businesses can quickly restore operations in the event of an attack and minimize downtime.

Conclusion - Moving Forward with Proactive Cybersecurity

Building a Culture of Cybersecurity Awareness

One of the most important aspects of proactive cybersecurity is building a culture of awareness within the organisation. Cybersecurity is not just the responsibility of the IT department; it requires the involvement and awareness of all employees. Regular training, updates on the latest cyber threats, and encouraging staff to adopt good security practices are all key components of building a resilient business.

A culture of cybersecurity awareness can help prevent the most common forms of attacks, such as phishing, by empowering employees to recognise suspicious activity and respond accordingly. Moreover, maintaining regular security assessments and keeping up to date with the latest developments in cybersecurity ensures that businesses stay one step ahead of potential attackers.

The Role of Techn22 in Supporting SMEs

At Techn22, we understand the unique challenges SMEs face when it comes to cybersecurity. We believe that every business, regardless of size, should have access to the tools, strategies, and expertise needed to defend against modern cyber threats. That’s why we offer a range of tailored cybersecurity services designed specifically for SMEs.

Whether it’s implementing dark web monitoring, phishing simulations, or providing Cyber Essentials certification support, Techn22 is here to help businesses safeguard their digital assets and build a strong security posture.

Secure Your Business with Techn22

As we move into 2025 and beyond, businesses must take cybersecurity seriously. The threats are real, and the consequences of inaction can be devastating. But by taking proactive steps today, SMEs can protect their operations, their data, and their reputation.

TECHN22

About Techn22: Your Cybersecurity and IT Partner

At Techn22, we specialise in providing small and medium-sized enterprises (SMEs) with robust, scalable IT support and cybersecurity solutions tailored to their unique needs.

The 2024 Cyber Threat Report highlights key risks like ransomware, phishing, and insider threats, and we're here to help businesses address these challenges with practical, affordable services.

From Cyber Essentials certification to dark web monitoring, phishing simulations, and penetration testing, we offer comprehensive services to enhance your business's security.

Contact Techn22 to safeguard your operations and achieve peace of mind in a complex digital landscape.

London Office

82 St John Street
London
EC1M 4JN

Preston Office

6 South Preston Office Village
Bamber Bridge
Preston.
PR5 6BL

General Enquiries

Tel: 0208 152 4000
Email: hello@techn22.co.uk

Support

Tel: 0208 152 4001
Email: support@techn22.co.uk

CREST PEN TEST

CYBER ESSENTIALS CERTIFIED

Microsoft Solutions Partner
Modern Work

TECHN22