Cyber Security in 2025

From ransomware and AI-powered attacks to supply chain vulnerabilities and the rise of quantum computing, the cyber security landscape is shifting rapidly. In this report, we unpack the key trends our experts foresee for 2025, their implications, and strategies to stay ahead of emerging risks.

Red
Helix

CONTENTS

"At Red Helix, we have seen another year of notable change. With evolving technologies and increasingly sophisticated attack methods, the need for adaptable, forward-looking security solutions is greater than ever. As we approach 2025, we remain dedicated to helping our clients navigate these complexities, focusing on resilience and innovation to stay ahead in an ever-shifting environment."

- Marion Stewart, CEO

1. Ransomware Remains the Biggest Threat

Ransomware remains a pervasive issue and will continue to grow as an attack vector in 2025. In the first three quarters of 2024, there were over 3,600 publicly reported ransomware victims, and this represents just a fraction considering that as many as 63% of ransomware victims are never publicly disclosed. Increasingly, attackers are targeting small and medium-sized enterprises (SMEs) rather than large, resource-rich organisations. With limited cyber security resources, SMEs are highly vulnerable, and cyber criminals see them as effective entry points into larger, connected organisations via their supply chains.

It is difficult to calculate the exact cost of ransomware as it varies per breach. Financial loss depends on the type of data encrypted/compromised, regulatory fines imposed, lost productivity in the aftermath of an attack, and the businesses' long term reputational damage.

The average extortion demand rose to £4.1 million per attack in early 2024, fuelling the rise of Ransomware as a Service (RaaS). This approach enables ransomware developers to sell code or malware on the dark web. RaaS providers offer various subscription models, from monthly toolkits to profit-sharing arrangements, providing easy entry points for hackers with limited technical skills. This commodification is making ransomware accessible to a wider criminal base, increasing both the volume and complexity of attacks.

This proliferation presents significant challenges for attribution and mitigation. Because RaaS separates ransomware developers from those deploying attacks, identifying specific actors has also become more challenging. Since RaaS allows affiliates to switch tools if an operator is caught, the risk is distributed across a resilient network.

The interplay between users and unpatched environments are often the most common sources of ransomware attacks. Both factors often serve as entry points for attackers, making them critical vulnerabilities in an organisation's defences. For example, if users operate in environments with outdated systems, the likelihood of successful exploitation increases significantly. Therefore, it is important organisations are prioritising these risks and have sufficient security measures to prevent ransomware.

Given the cost and difficulty of responding to ransomware attacks, preventive strategies are crucial. Regular patching, data backups, network segmentation, and up-to-date Endpoint Detection & Response (EDR) systems are essential. Organisations should also foster a culture of cyber security awareness through regular testing and training. In this high-risk environment, effective protection strategies will increasingly outweigh reactive measures like insurance, as these only address the aftermath rather than preventing breaches.

2. Recognising the Strengths and Threats Posed by AI Adoption

In accordance with the Gartner Hype Cycle trajectory, AI technology appears to be approaching the 'Slope of Enlightenment'. With businesses rapidly adopting it as they recognise its potential. An Ernst & Young study found that **95% of senior executives are already investing in AI**.

AI represents both an opportunity for efficiency and a growing internal security challenge, with organisations balancing access to new technology with robust protections.

The malicious use of AI, however, is evolving rapidly. Hackers are leveraging AI for automated, more sophisticated phishing schemes, social engineering, deepfakes, and even malware generation. Throughout 2025, the volume, complexity, and effectiveness of attacks will intensify, demanding agile countermeasures.

Deepfakes are a prime example of AI exploitation. One recent case involved **cyber criminals using deepfake technology to impersonate a CFO on a video call**, resulting in a $25 million fraudulent transfer. Gartner predicts that **by 2026, nearly one-third of enterprises will view traditional identity verification as unreliable** due to AI-generated deepfakes.

Another threat is data poisoning, where attackers manipulate the data used to train AI systems, influencing the AI's behaviour, or degrading its performance. This subtle manipulation is particularly dangerous as it can corrupt AI-driven insights without being immediately detectable.

In response, security teams are increasingly using AI to detect and mitigate sophisticated threats, automate vulnerability scanning, and to handle vast amounts of security data. This proactive use of AI will allow cyber security teams to focus on higher-value tasks, while the technology detects potential issues early.

The assertion that AI can be a force for good in combating cyber threats is demonstrated by innovations like Telefonica's AI-powered tool "Daisy," which targets and entraps scammers. This example highlights the growing potential of artificial intelligence to proactively address challenges in the cyber domain. As cyber threats grow more sophisticated, cyber security experts, AI developers, and policymakers will likely collaborate more frequently to create original solutions that safeguard digital ecosystems while reinforcing the positive narrative of AI as a problem-solving technology.

3. Building a Resilient Supply Chain

As businesses become more digitally intertwined within their supply chains, the frequency of supply chain cyber breaches has increased significantly. This trend is not going to subside in 2025, making supply chain security a topic of growing importance. As businesses expand and outsource, they often lack comprehensive monitoring and understanding of all third-party connections, leaving these entry points vulnerable.

Most companies monitor only 30% of their third-party connections, creating opportunities for cyber criminals. SMEs, constrained by budgets and often lacking cyber security expertise, are common targets in supply chain attacks. As larger businesses tighten their security, attackers are increasingly exploiting SMEs to bypass the strong security postures of their target enterprises. Consequently, large companies will demand stricter security measures from their suppliers. As software supply chain attacks are expected to rise in 2025, the importance of strong cyber security protocols, regular training, and thorough monitoring of third-party interactions is vital.

As the supplier selection process matures, more companies will make cyber security measures mandatory. It is important that your supply chain is sufficiently prepared, or you may lose out on potential customer/vendor relationships. This is already prevalent in the financial sector and is fast becoming the norm across all industries as cyber is increasingly recognised for the value it adds to organisations winning new contracts.

> ***“Supply chain security is particularly important. It only takes one member of your supply chain to suffer a breach for far reaching consequences. We take our due diligence and checks very seriously when we are working with new vendors to ensure our supply chain remains secure”.***
>
> **- Duncan Forrest, IT Director**

4. Phishing Remains the Main Attack Vector

Phishing has persisted as a **top cyber threat for over a decade**, remaining a **widespread and costly attack vector**. As we advance into 2025, the methods and technologies behind phishing are expected to evolve, increasing in sophistication to overcome current security measures.

An increasing concern is the commercialisation of phishing through 'toolkits' that attackers can purchase. These toolkits, often targeting identity information, have exacerbated phishing risks, with identity and credential compromises involved in **80% of phishing incidents**.

A particular phishing technique known as adversary-in-the-middle (AitM) has gained traction, circumventing traditional defences like multifactor authentication (MFA) and Endpoint Detection & Response (EDR). AitM phishing toolkits, including Modlishka, Muraena, and Evilginx, create a reverse proxy between a target and a legitimate website. The attacker intercepts communications, collecting sensitive data while the user remains unaware. This approach bypasses user vigilance by creating seemingly authentic web pages, allowing attackers to capture login credentials and other critical information.

Cyber criminals are expanding their methods with emerging types of phishing, such as quishing, smishing, and vishing. Quishing leverages QR codes embedded with malware, which, when scanned, can compromise a target's device. Smishing and vishing use SMS and video calls, respectively, to deceive users into disclosing sensitive data. With personal devices increasingly holding sensitive information, the success rates of these new phishing vectors continue to grow. These variations retain phishing's core objective, exploiting user trust to gather sensitive information. As these newer techniques gain prominence, user awareness must grow to mitigate their impact.

5. Do Not Underestimate the Importance of Your Security Culture

A strong security culture is front and centre of how a business to combat these evolving threats. Comprehensive education initiatives that focus on real-world risks and emphasise the importance of individual actions in preventing breaches. Integrating cyber security risks into the business risk management processes is key to driving awareness and mitigation strategies from the C-suite. By embedding cyber security awareness into everyday business practices and fostering a culture where every employee understands their role in maintaining digital safety, organisations can significantly reduce their vulnerability to human-centric attacks. As cyber threats continue to evolve, the importance of a strong security culture cannot be overstated.

Building a culture of security awareness requires comprehensive education initiatives, focusing on real-world risks and the importance of individual actions in preventing breaches. However, there remains a gap in training adherence, with a 2024 State of Sysadmin report showing that **11% of IT professionals skip required training.**

As cyber security technology advances, the importance of human awareness is increasingly evident, driving organisations to invest in behaviour-driven security measures. These include using behavioural analysis to identify unusual patterns, fostering collaboration within security teams, and embedding cyber security within organisational health and safety frameworks. Continuous training and AI-powered tools can support analysts in threat detection, while collaborative environments enable the sharing of insights critical to investigations.

With cyber security's evolving role, many organisations now view it as a 'health and safety' issue essential to business operations. The National Cyber Security Council report that **more ransomware incidents result from poor cyber hygiene than sophisticated attack techniques**. This emphasises the importance of maintaining robust cyber security practices. Consequently, cyber security decisions are now part of executive-level discussions, emphasising preventive measures as essential.

Continuous risk assessments now serve a role akin to physical safety audits. These assessments help identify vulnerabilities and enable proactive threat responses, protecting digital assets and employee productivity. This focus on cyber security as part of an organisation's 'health and safety', promotes a resilient, proactive culture that minimises human risk factors, embedding cyber security awareness into everyday business practices.

11% of IT professionals skip required training.*

*According to the 2024 State of Sysadmin Report

6. Multi-Domain Security Across IoT and Cloud Environments

The convergence of Internet of Things (IoT) and cloud computing has created a complex, interconnected ecosystem that demands a comprehensive multi-domain security approach. As IoT devices proliferate, and with growth projections exceeding 21 billion by 2025, each connected device introduces potential vulnerabilities that span both the physical and digital realms.

Simultaneously, the widespread adoption of cloud infrastructure increases organisations exposure to risks such as data breaches and unauthorised access.

This interconnected landscape necessitates a holistic security strategy that addresses the unique challenges of both domains while recognising their interdependencies. Effective multi-domain security must consider the entire data lifecycle, from IoT device-level authentication to cloud-based storage and processing. Organisations need to implement robust encryption protocols, to secure data transmission between IoT devices and cloud platforms.

Additionally, adopting a shared responsibility model for security becomes crucial, with both cloud service providers and customers playing active roles in maintaining data integrity and confidentiality. The integration of artificial intelligence (AI) and machine learning (ML) technologies further enhances the capability to detect and respond to threats across both IoT and cloud environments.

These advanced tools can analyse vast amounts of data from diverse sources, identifying patterns and anomalies that might indicate security breaches. As the attack surface expands with the growth of IoT and cloud adoption, organisations can capitalise on continuous monitoring, regular security assessments, and the implementation of adaptive security architectures to ensure they keep pace with emerging threats.

> *"As more IoT devices are introduced, the complexity of managing the networks grows. This isn't only a matter of scale; it also stems from the diversity of devices being integrated. Each device can come with its own operating system, along with varying protocols, standards, and security measures – which can ultimately lead to vulnerabilities and complications in protecting the network."*
>
> **- Rob Pocock, Technology Director**

7. Stricter Compliance Regulations

Expectations of basic cyber practises are being raised industry wide, as we see the introduction of GDPR for businesses. This requires the implementation of strict data privacy practices, providing clear data usage disclosures and the necessity of obtaining user consent. Cyber Essentials is also an important framework for ensuring a minimum level of cyber security. It acts as a simple and accessible framework, to help organisations of all sizes and industries protect themselves against common cyber threats. By focusing on basic security hygiene, it aims to significantly reduce the risk of cyber-attacks.

Tightening compliance regulations, including the NIS2 Directive and the EU's Digital Operational Resilience Act (DORA), are reshaping organisational cyber security. The NIS2 Directive mandates higher standards for essential service providers, including accountability for executives and significant penalties for non-compliance. Executives now face direct economic responsibility if a breach occurs under their oversight, leading to a shift in cyber security decision-making at the board level. PwC's 2025 Global Digital Trust Insights Survey, reported that **96% of executives claimed regulatory requirements are a key factor in prompting investments** for bolstering security measures.

DORA introduces comprehensive requirements for financial institutions to bolster risk management, incident reporting, and third-party provider oversight. This regulatory shift underscores the need for proactive risk management and supply chain security, with compliance increasingly becoming integral to business resilience. **Over 75% of executives recognise that compliance with new regulations has improved or matured their cyber security posture.**

As compliance expectations rise, cyber insurance costs are projected to increase, with insurers requiring proof of strong cyber security practices. The Cybersecurity Maturity Model Certification (CMMC) 2.0, for example, requires contractors to meet stringent standards, pushing businesses large and small to strengthen their security measures.

"Regulatory frameworks like NIS2 and DORA are driving a fundamental shift in how organisations approach cyber security. With executives now directly accountable for breaches, cyber security is no longer just an IT concern—it's a boardroom priority."

- Tom Exelby, Head of Cyber Security

8. The Zero Trust Model for the Hybrid Work Era

In recent years, the rise of hybrid and remote work has introduced new security challenges, prompting businesses to adopt more sophisticated security measures. By 2025, we expect even greater investments in security solutions specifically tailored for remote work environments, particularly in technologies like Virtual Private Networks (VPNs) and Secure Access Service Edge (SASE). These tools are critical for providing secure, flexible access across varied work settings, supporting a ‘work from anywhere’ culture while safeguarding sensitive data.

As cyber threats, such as ransomware and network breaches, continue to escalate, the need to limit attack impact has pushed the Zero Trust model into the cyber security spotlight. Zero Trust’s foundational principle, ‘never trust, always verify’, offers a structured, proactive approach to minimise risk by restricting lateral movement across networks. By requiring continuous authentication and enforcing least-privilege access, organisations can significantly reduce exposure, granting users access solely on a ‘need-to-know’ basis.

As cloud adoption accelerates, Zero Trust architectures are solidifying as core components of modern Security Operations Centres (SOCs). This model is especially critical for managing risks associated with remote access and potential insider threats in the cloud era. Key Zero Trust strategies, such as continuous identity verification, micro-segmentation, and least-privilege access, fortify defences against both external and insider threats, ensuring robust security across digital environments.

Emerging methodologies like micro-segmentation are helping organisations reduce the potential fallout of a cyber incident. By dividing networks into isolated segments, micro-segmentation prevents threats in one area from cascading across the entire system. Each segment operates autonomously, ensuring that a breach in one segment has minimal impact on other parts of the network.

Zero Trust Network Access (ZTNA) has proven invaluable in overcoming cyber security challenges within hybrid work settings. By advancing traditional VPN capabilities, ZTNA ensures that remote access remains secure, supporting a dynamic workforce while mitigating risks in multi-cloud environments.

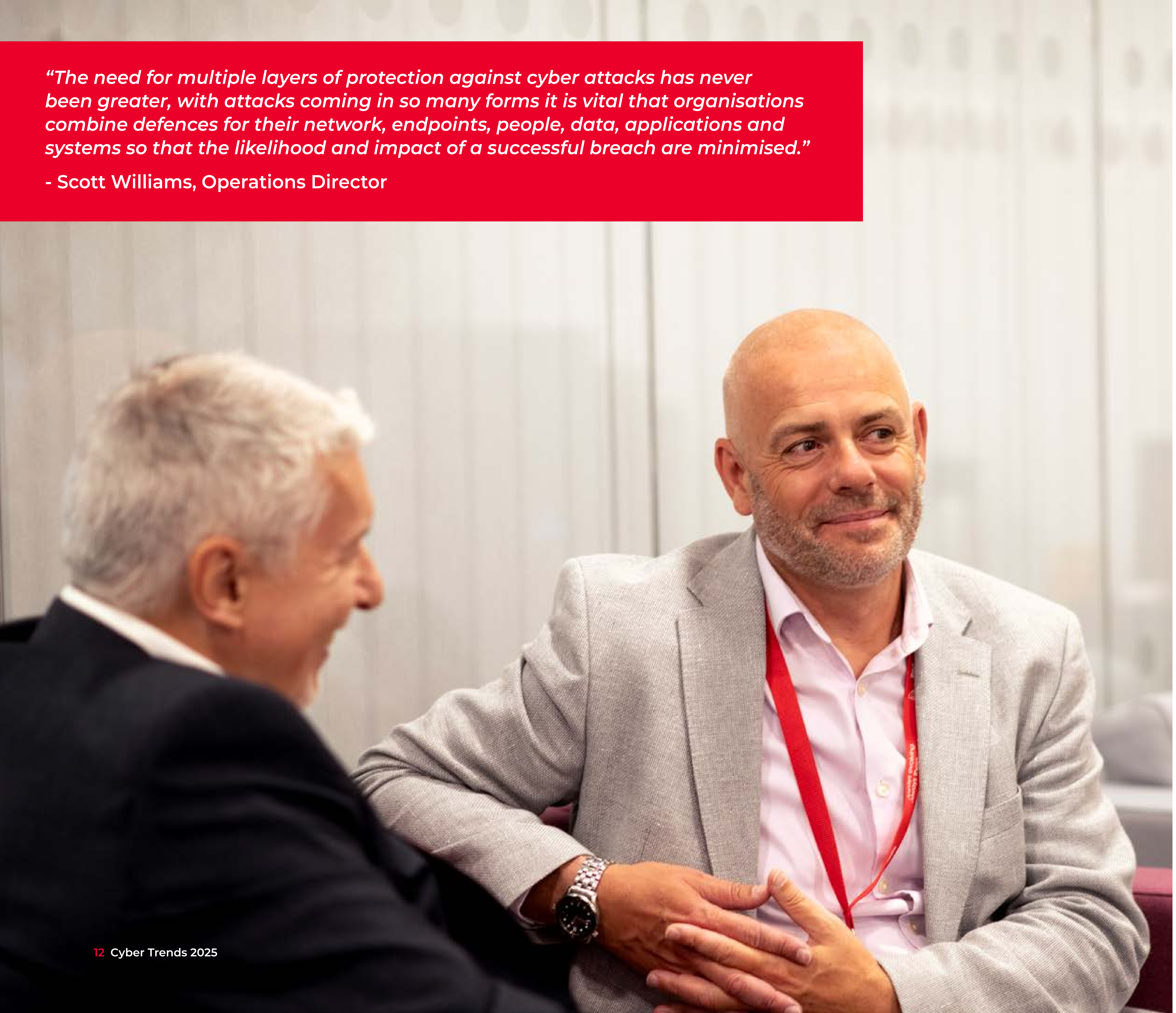
As cyber security strategies advance, Zero Trust is poised to become the backbone of resilient, adaptive cyber security in 2025.

9. Quantum Computing and Changing Methods of Decryption

As quantum computing technology advances, it presents a significant threat to existing encryption methods, which form the foundation of modern cyber security. Traditional encryption methods, such as the widely used AES256, are designed to secure sensitive data by making decryption a time-consuming process that typically takes years. However, quantum computers, with their ability to perform complex calculations at exponentially faster rates, could potentially break current encryption standards in a matter of hours rather than decades.

While quantum computing is not yet mainstream, the research and development in this area is advancing rapidly. Cyber criminals are already exploring ways to use quantum computing to improve the speed and effectiveness of their attacks. This makes it increasingly crucial for organisations to prepare for the 'quantum era' by developing quantum-resistant cryptographic algorithms. The need for post-quantum cryptography will become more pressing as quantum technology becomes more accessible.

As quantum computing continues to progress, businesses must stay agile and innovative in adopting recent technologies to defend against future cyber threats. This proactive approach will be key to securing sensitive data and maintaining trust in digital systems.



“The need for multiple layers of protection against cyber attacks has never been greater, with attacks coming in so many forms it is vital that organisations combine defences for their network, endpoints, people, data, applications and systems so that the likelihood and impact of a successful breach are minimised.”

- Scott Williams, Operations Director

10. A Comprehensive Approach is Needed

As we look towards the future of cyber security in 2025 and beyond, both established and emerging threats will continue to evolve, demanding greater attention, innovation, and preparedness from organisations.

The convergence of persistent threats, emerging technologies, and regulatory changes underscore the need for businesses to take a comprehensive approach to cyber security. This means investing in the development of human expertise, adopting innovative technologies, and ensuring compliance with evolving standards.

As cyber threats continue to grow in complexity, organisations must remain agile, innovate in their defence strategies, and stay prepared for both current and future risks to ensure their organisation can continue to operate and thrive.

For additional support and expert guidance, cyber security specialists such as Red Helix can assess your current security measures and advise you on adopting the strategies and solutions necessary for comprehensive protection.

For specific security concerns or to explore how to better safeguard your company, employees, and clients, please contact Red Helix for a complimentary, no-obligation consultation.

Visit www.redhelix.co.uk/contact and one of our team will be happy to assist you.