Picture credit: AdobeStock

NAVIGATING EVOLVING THREATS

Anthony Young *outlines why 2025 will be a challenging year for cyber security*

Few industries evolve as fast – or as unpredictably – as cyber security and 2025 will be no exception. The year ahead promises advances in AI-driven attack strategies, heightened regulatory demands, and escalating threats targeting critical infrastructure. To stay ahead, organisations must balance innovation, resilience and adaptability, ensuring their defences keep pace with an ever-changing landscape.

This article consolidates insights from key experts within Bridewell to outline emerging trends and strategies, offering a forward-looking perspective on cyber security for the year ahead.

RESILIENCE WILL DEFINE SUCCESS

The pace of cyber threats is evolving rapidly, with geopolitical tensions driving a surge in incidents that can disrupt critical infrastructure and key services. Nation-states are adopting increasingly sophisticated cyber tactics, ranging from targeted, long-term espionage to disruptive ransomware operations aimed at destabilising critical services. Additionally, disinformation campaigns powered by AI-generated fake news are posing new challenges, eroding public trust and social stability by spreading misinformation that can sway public opinion.

At the organisational level, cyber security teams are under increasing strain. Budget reductions, heightened compliance demands and an overwhelming array of risks are stretching resources thin. Adding to the pressure, enforcement notices for NIS non-compliance are expected to proliferate throughout 2025 and 2026, leaving little room for error.

The urgency to comply can leave organisations vulnerable to opportunistic vendors. These vendors may offer quick-fix compliance solutions, but lack a thorough, long-term understanding of complex security needs. Compounding these challenges, there remains an industry-wide shortage of cyber security skills, particularly in key areas such as security architecture and OT (Operational Technology) security. These skill gaps are creating vulnerabilities that cyber criminals and nation-states alike may exploit if organisations fail to shore up their internal capabilities.

Cyber security teams must not only be prepared to deploy new defences, but also to reassess existing security frameworks to ensure that they remain effective

To bolster resilience, organisations should focus on a multifaceted approach: upskilling internal teams, thoroughly vetting vendor claims and prioritising long-term partnerships with trusted providers. Building a resilient cyber security strategy now will empower organisations to face not only today's threats but also prepare for future challenges as the threat landscape continues to evolve.

AI'S EVOLUTION

AI's presence in cyber security will only grow in 2025, both as a tool for threat actors and as a defence mechanism. Cyber criminals are increasingly leveraging AI to craft more sophisticated phishing schemes, perform impersonations with greater precision and automate attacks on a larger scale.

This raises fundamental security questions, particularly in verifying the authenticity of virtual interactions – a challenge that many organisations are struggling to address. AI-based tools can now mimic a person's voice, facial expressions or writing style, making it easier for attackers to deceive individuals or gain unauthorised access to sensitive information.

State-sponsored groups are using AI not only to enhance the effectiveness of their attacks, but also to scale them. By targeting critical infrastructure with AI-powered exploits, attackers can identify and take advantage of zero-day vulnerabilities, potentially disrupting essential services. These threats have serious implications for sectors such as finance, healthcare and energy, where any significant disruption could result in cascading effects, impacting both organisations and the communities they serve.

Defending against these risks will require an equally advanced AI-driven defence approach. Machine learning and pattern recognition technologies can detect anomalies and suspicious patterns early, allowing cyber security teams to respond to threats more rapidly and effectively.

However, AI-based tools are most effective when combined with human oversight, as cyber security professionals bring critical judgment and contextual understanding that automated systems lack. Streamlining security infrastructures and integrating AI-driven tools into cohesive frameworks will allow security teams to stay ahead of increasingly sophisticated threats, balancing the advantages of automation with the essential insights that only experienced professionals can provide.

TAILORED APPROACHES

The role of commercial teams in cyber security is evolving as businesses seek solutions that are both cost-effective and tailored to specific organisational needs. Economic pressures have led many organisations to shift away from traditional, long-term contracts in favour of flexible, short-term agreements. This shift is particularly evident in industries such as construction, engineering and government, where budgets are often tight, and the ability to adapt quickly to changing needs is crucial.

Commercial teams are helping clients understand not only the technical aspects of cyber security solutions, but also the broader economic impact of their decisions. By emphasising the importance of customisation, commercial teams enable organisations to align their security investments with both immediate priorities and longer-term goals, helping them achieve a balance between financial sustainability and robust security.

Flexible contracts also provide organisations with greater control, allowing them to scale or adapt their cyber security services as their needs evolve. For service providers, this trend highlights the importance of delivering adaptable, forward-thinking solutions that can be easily tailored to meet diverse requirements. Providers who focus on flexibility and client education will be better positioned to serve an evolving market, helping organisations maintain resilience even as security threats and economic conditions change.

> IT'S IMPORTANT THAT CYBER STRATEGIES ARE EVERY BIT AS ADAPTABLE AS THEY ARE ROBUST

CLOUD ADOPTION

The adoption of cloud solutions in OT (Operational Technology) environments will continue to gain momentum in 2025, especially as organisations seek to optimise their cyber security investments. Many businesses have made substantial investments in tools such as Network Detection and Response (NDR) systems, only to find that these technologies do not fully meet their expectations due to a lack of operational maturity or an incomplete integration into the broader security ecosystem.

This disconnect between investment and return is prompting organisations to rethink their approach to security in OT environments, leading many to consider hybrid cloud models that offer greater flexibility, control and redundancy. Hybrid cloud solutions allow organisations to combine the agility and scalability of cloud-based services with the vigorous security measures needed to protect sensitive OT assets, such as those managing critical infrastructure.

In OT environments, the push towards cloud solutions also reflects a growing emphasis on adopting tools that provide clear, measurable risk reduction rather than a broad array of features that may go underutilised. Many organisations are now moving away from legacy systems in favour of cloud-first approaches, which allow for enhanced control and more seamless integration of new technologies. However, adopting cloud in OT environments requires a mature, risk-focused approach, as operational disruptions in these settings can have serious, far-reaching consequences.

To stay ahead, businesses must evaluate their current cyber security investments and focus on solutions that bring real-world value. By prioritising hybrid cloud models and implementing mature, well-integrated security practices, organisations can better position themselves to handle the operational challenges that lie ahead, gaining the flexibility to adapt their security measures as new risks emerge.

TOUGHER REGULATIONS

With the introduction of regulatory frameworks such as NIS2 in the EU and the Digital Operational Resilience Act (DORA), regulatory compliance will be a key focus for organisations in 2025. Additionally, anticipated UK legislation will extend cyber requirements to new sectors, including energy, healthcare and finance, broadening the scope of regulations across various industries. As a result, companies operating internationally will face increasing scrutiny and pressure to align with complex, often overlapping regulatory standards.

AI-BASED TOOLS ARE MOST EFFECTIVE WHEN THEY ARE COMBINED WITH HUMAN OVERSIGHT

In the energy sector, meeting the enhanced CAF (Cyber Assessment Framework) profile by 2027 will be a significant undertaking, requiring organisations to overhaul their compliance efforts proactively. Delaying action is no longer a viable option, as escalating fines and expanded regulatory authority make a reactive approach too risky. Beyond financial penalties, non-compliance can lead to reputational damage, operational disruptions and strained relationships with regulators, all of which can hinder long-term organisational stability.

The ongoing shortage of skilled cyber security professionals, particularly in OT and AI-driven defence roles, adds another layer of complexity, making it challenging for organisations to implement effective compliance programs. Businesses should prioritise early compliance efforts and secure specialised talent to navigate this complex and evolving regulatory landscape.

RAPID INNOVATION

Rapid technological advancements will continue to reshape the cyber security landscape in 2025, with the pace of innovation accelerating faster than ever.

The rise of generative AI in recent years has shown how swiftly new tools can be adopted and weaponised, creating both opportunities and threats for cyber security professionals. As new technologies emerge, organisations must prepare to adapt quickly, recognising that these shifts can bring as many risks as they do benefits.

Quantum computing is one of the most anticipated and potentially disruptive technologies on the horizon. Although widespread implementation may still be a few years away, its potential to break modern cryptographic standards represents a substantial threat to cyber security. Quantum's capability to decrypt data that is currently secure could fundamentally alter the landscape, leaving systems and networks vulnerable to attacks unless organisations begin preparing now.

In this environment of rapid change, staying ahead of technological developments is essential. Cyber security teams must not only be prepared to deploy new defences but also to reassess existing security frameworks to ensure they remain effective. Having forward-facing teams dedicated to evaluating speculative advances and weighing potential risks and benefits will enable organisations to stay agile, making the most of emerging tools while mitigating the vulnerabilities they may introduce.

As businesses face a confluence of geopolitical tensions, economic pressures and evolving regulatory demands, organisations must carefully consider how they'll review their cyber security strategies for 2025.

To succeed, organisations should integrate cutting-edge technologies, like AI and machine learning, with traditional human expertise, ensuring that cyber security strategies are as adaptable as they are robust. Additionally, fostering collaboration between commercial and technical teams will be crucial, helping organisations align security strategies with broader operational and financial goals. Staying ahead of regulatory changes will also be essential, as proactive compliance not only mitigates risks but also builds a strong foundation for resilience in an increasingly scrutinised environment.

By focusing on long-term value, prioritising adaptability and nurturing a culture of continuous improvement, organisations can position themselves to navigate the evolving cyber security landscape of 2025. With a forward-thinking, agile mindset, they will be well-equipped to face emerging risks head on and capitalise on new opportunities to strengthen their cyber security posture, building a resilient foundation for the future ●

ANTHONY YOUNG is CEO at Bridewell.

Cyber criminals are increasingly leveraging AI to craft more sophisticated phishing schemes, perform impersonations with greater precision and automate attacks on a larger scale

Picture credit: AdobeStock