waystone | Compliance Solutions

Cyber security trends to watch in 2025 – predictions and preparations

John Zuska

December 3, 2024

As 2024 draws to a close, the cyber security landscape continues to evolve at a rapid pace. Businesses, governments, and individuals face new challenges and opportunities as they strive to secure their digital environments. For December's blog topic, we will be looking ahead to 2025 and significant changes driven by emerging threats, technological advancements, and shifting regulatory frameworks.

Here are the key trends to watch and prepare for in the coming year:

1. AI-driven cyber threats and defenses

Artificial Intelligence (AI) will remain a double-edged sword. Cyber criminals are expected to refine AI-powered tools for automating phishing attacks, breaking CAPTCHA systems, and identifying vulnerabilities. On the defensive side, AI-driven threat detection and response tools will become even more sophisticated, leveraging predictive analytics and machine learning to identify anomalies in real time. Businesses will need to stay ahead by adopting advanced AI defenses while preparing for AI-driven attacks.

Preparation tip: invest in AI-powered security solutions that offer real-time monitoring and analysis, and train employees to recognize AI-enhanced social engineering attempts.

2. Quantum computing's security implications

Quantum computing, while still in its nascent stages, poses a long-term challenge to traditional encryption methods. In 2025, we may see significant progress in quantum computing technology, prompting a shift toward quantum-resistant cryptographic algorithms.

Preparation tip: begin assessing cryptographic systems and planning for a transition to quantum-safe encryption standards as they become available.

3. Cyber insurance evolution

As ransomware attacks and data breaches persist, the cyber insurance market will evolve to address growing risks. Expect stricter underwriting requirements and higher premiums as insurers refine their risk assessments.

Preparation tip: review your coverage and coverage amounts. Ensure ransomware is covered and a rider, if necessary, is created. The amount will be on the higher side for firms that store more data. If you have an internal development team or internally developed applications, review total data usage with your team to ensure you have sufficient coverage.

4. Regulatory and compliance shifts

Governments worldwide are tightening regulations to address privacy and cyber security concerns. In 2025, businesses should anticipate new compliance requirements, particularly in data protection and critical infrastructure security.

Preparation tip: even if you are a newly-formed firm, be sure to have polices in place. It's far easier to create them at the beginning than to change behaviors once a firm is established. They will be required soon, so it's best to prepare as early as possible.

5. Focus on zero trust architecture

Zero trust principles will dominate cyber security strategies in 2025 as organizations move away from perimeter-based security models. The "never trust, always verify" approach will help mitigate risks associated with remote work and cloud adoption.

Preparation tip: transition to a Zero Trust framework by implementing multifactor authentication (MFA), least privilege access, and continuous monitoring.

6. Human-centric cyber security

Despite advances in technology, the human factor remains a critical vulnerability in cyber security. In 2025, the focus will intensify on reducing risks stemming from human error, insider threats, and insufficient awareness. Human-centric cyber security recognizes that effective defenses depend not just on tools and protocols but also on empowering people with the right knowledge, habits, and support systems. With humans remaining the weakest link in cyber security, there will be a renewed focus on training, awareness, and user-friendly security tools.

Preparation tip: regularly review access permissions and ensure employees only have access to the resources that they need to perform their role. This is especially important for executives who have far more control than is truly necessary.

Preparing for 2025

The cyber threat landscape is dynamic and unforgiving, but with proactive measures, organizations and individuals can stay ahead. By understanding these emerging trends and adapting strategies accordingly, we can approach 2025 with confidence, resilience, and a commitment to securing our digital future.

Waystone Compliance Solutions is a leading provider of cyber security consulting and compliance services to the financial services industry. If you would like to find out how Waystone can help you to assess your current cyber security measures, please reach out to your usual Waystone representative, or contact us below.

Get in touch →