7 Cybersecurity Predictions for 2025

By Thomas DeMayo, Partner, Nick DeLena, Partner and Robert Gaines, Director

In 2024, we saw a rapid increase in cybercrime, surmounting the list of concerns for business leaders. A *CFO Magazine* survey found that ransomware attacks were the number one concern of the C-Suite. Additionally, 45% of cybersecurity leaders identified cyber incidents as the most feared cause of business interruption. These fears are well-founded. Last year, cybercrime damages reached $9.5 trillion globally, the global average data breach cost was $4.88 million (up 10%), phishing emails surged 1,265% and cyberattack frequency was up 30% across all industries.

Driven by the rapid weaponization of new technologies and techniques, we expect threats to the cybersecurity landscape will continue at a staggering pace in 2025. Here we offer seven predictions covering trends and developments in cybercrime, organizational priorities and the regulatory environment as your business prepares its cybersecurity strategies for 2025.

The Past is Prologue

Looking at the past to prepare us for the future, 2024 exposed weaknesses in business cybercrime defense across a few key areas: third parties, supply chains, resiliency and software-as-a-service (SaaS dependencies). We anticipate threat actors will continue targeting these areas in 2025, with artificial intelligence (AI) adoption and utilization leading the charge. Read on for our 2025 predictions.

1. Malicious Use of AI in Cyber Attacks

AI will continue to equip entry-level cyber criminals with highly advanced and accurate hacking tools and platforms, enabling more individuals to launch attacks. We expect sophisticated AI attacks that can craft an entire attack chain — including profiling targets, generating malware, delivering payloads, performing lateral movement across the network and exfiltration of discovered data. Defenses against these autonomous attack methods must be layered and equally sophisticated to prevent, detect, respond and recover.

2. A Rise in Deepfake Social Engineering Attacks

AI can leverage public or leaked user data with deepfake technology to make an attacker look and sound authentic. This will increase the effectiveness of social engineering attacks using phone, text and video. AI will also drive a rise in “reverse data theft” where stolen breach data is used to create false digital identities that are difficult for organizations and end-users to differentiate between real and fake personas. Expect to see this increasingly in social media forums where attackers strive to appear legitimate to establish connections with users. This will result in more realistic social engineering attacks that make validating users and customers difficult for support teams, customer service and automated support mechanisms. For this reason, the use of voice as an authentication mechanism will likely become obsolete.

3. Attacks Against Third Parties and Supply Chains

Attackers will continue to look for methods to infiltrate software supply chains and insert malicious code into trusted libraries. With companies using an average of 371 SaaS apps (per *Productiv*), most

organizations do not have proper visibility into their supply chain and, consequently, don't know how to respond to a cyber-attack on one of their third parties. Attackers rely on these blind spots to infiltrate businesses and keep persistence within the environment. Defense against supply chain attacks requires proper cyber hygiene, monitoring for behavioral changes in users and applications (heuristics) and proper due diligence prior to implementing a new solution and periodically thereafter.

4. Advanced Privilege Escalation Attacks

Attacks of this nature exploit poorly configured settings within the identity and access management (IAM) components of software — especially within the complex cloud-based and hybrid environments now a dominant feature of most business architectures. A hybrid environment includes both traditional on-premise applications and cloud applications. The proliferation of applications combined with inconsistent or poorly managed access controls will inevitably result in more attacks. Additionally, misconfigured single sign-on (SSO) systems or hybrid infrastructures that have incorrect dependencies or misconfigured trust relationships can be equally exploited using similar methodologies.

5. Integration Between Cyber Resilience and Business Continuity

Major service disruptions in 2024 from CrowdStrike, AT&T and Microsoft 365 introduced businesses to the complexities of managing third parties that control or are a critical dependency for their operations. This wake-up call has businesses focusing on resilience solutions so that they can continue to function despite cyber incidents and application outages, combining business continuity with incident response operations. In a regulatory response to ensure resiliency in the EU's financial sector, the Digital Operational Resilience Act (DORA) was enacted on January 7, 2025. It is designed to manage information and communication technology (ICT) risks, placing heavy emphasis on business resilience, especially regarding third-party service providers that ICT relies on for operations. All businesses should embrace ensuring robust resiliency in 2025 as a key goal.

6. Evolution of the CISO Role

The role of the Chief Information Security Officer (CISO) will further transform from a technical specialist to a strategic leader as business operations and cybersecurity continue to converge and the need to communicate cyber risk in terms of business impact becomes indispensable. The role of the CISO will take on more responsibilities for regulatory compliance as pressures around incident response, cyber resilience and accountability continue to increase. Talent shortages in this area are expected to persist in 2025 and beyond. We anticipate greater reliance on virtual CISOs (vCISOs) to fill critical roles for organizations.

7. Increasingly Stringent Regulatory Environment

We expect the regulatory landscape for cybersecurity and data privacy to become significantly more complex in 2025, presenting businesses with a multitude of challenges.

- DORA will mandate rigorous IT risk management and incident-reporting protocols for organizations operating in the EU financial sector.
- The Cybersecurity Maturity Model Certification (CMMC) will require robust cybersecurity practices to protect controlled unclassified information for those doing business in the U.S. defense sector.
- Several U.S. states (including Texas, Oregon, Florida, Montana, Minnesota and Rhode Island) will have comprehensive data-privacy laws in full effect, demanding stringent data-protection and consumer-rights management.
- The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) rule is expected to become final in 2025. It will mandate very strict cybersecurity incident reporting to companies in critical infrastructure sectors.

A Forward Look

Our cybersecurity predictions for 2025 emphasize the importance of proactive, adaptive and layered defenses to counteract increasingly complex threats. As attackers leverage AI with aggregate breach data to create convincing deepfakes and launch sophisticated autonomous attacks, organizations must invest in resilience through risk management, third-party due diligence, advanced detection systems and improved supply chain management. The evolving role of the CISO, alongside the integration of cybersecurity into business continuity strategies, underscores a new long-term shift where security is no longer a technical issue managed in isolation but a critical component of business operations. By understanding these trends and taking action now, businesses can adequately defend themselves against anything 2025 throws their way.

Contact Us

Our team at PKF O'Connor Davies serves as trusted cybersecurity advisors to many companies and boards. We welcome the opportunity to answer any questions you may have on this topic or other matters relative to cybersecurity and privacy. Please reach out to any of the Cybersecurity and Privacy Advisory team members below:

Thomas J. DeMayo, CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
Partner
Cybersecurity and Privacy Advisory
tdemayo@pkfod.com | 646.449.6353

Nick DeLena, CISSP, CISA, CRISC, CDPSE, CMMC-CCP
Partner
Cybersecurity and Privacy Advisory
ndelena@pkfod.com | 781.937.5191

Robert Gaines, CISSP, CECI, CCFI, C|OSINT
Director
Cybersecurity and Privacy Advisory
rgaines@pkfod.com | 425.518.1974