Computer Emergency Response Team of Mauritius

Cyber Security Trends and Threats to Watch Out for 2025

Date of Issue: 23 January 2025

As the threat landscape grows, predicting cyber security trends 2025 becomes more important. These emerging issues range from AI-driven malware to concerns about quantum computing and require forward-thinking strategies. Below, some cybersecurity trends and threats are highlighted that could change digital defenses in the next few years. Understanding the motivations behind these latest cyber security trends will help businesses adapt their tools and training to not be left behind. To that end, let's take a closer look at each trend, explaining why it matters and how organizations can respond.

1. AI-Driven Malware

Machine learning is now being used by criminals to mutate malicious code in real-time to avoid being statically detected. As a result, this technology enables malware to deepen its installation, detect sandbox environments, and adapt to endpoint defenses. Manual threat hunting is outdated by AI-based infiltration, so defenders have to use advanced anomaly detection. Cyber security trends reveal that zero-day attacks, enabled through the use of automated tooling, are the most urgent threats.

2. Zero Trust Architectures

With perimeter-based security becoming obsolete, zero trust becomes the new hot thing. Zero trust gives blanket access only after initial authentication and then revalidates every request. Against the backdrop of lateral movement, a hallmark of advanced breaches, this approach provides an important option for defenders. Zero trust is one of the top cyber security trends in 2025, with more and more organizations adopting micro-segmentation, user context checks, and continuous session monitoring

3. Quantum Computing Threats

While mainstream yet, quantum computing has the potential to break contemporary encryption. Today, intercepted data may be stockpiled by cybercriminals or nation-

states in the hope that they can decrypt it with quantum hardware in the future. Latest trends in cyber security discussions lead to quantum-resistant algorithms for critical data. By adopting post-quantum cryptography early, you'll be safe when quantum machines reach maturity.

4. Ransomware-as-a-Service Evolution

More and more ransomware groups are turning into service providers, providing affiliates with easy-to-use toolkits for a cut of the profits. This reduces the barrier to skill, creating a surge of attacks that weaken organizations and demand large payouts. RaaS has been flagged by many experts as a focal point within the cyber security trends 2025, with cost of recovering from a ransomware attack now averaging USD 2.73 million, according to research data. As such, offline backups and segmented networks become necessary resilience strategies.

5. 5G and Edge Security Risks

With 5G networks taking off, data volumes increase, and real-time use cases extend to IoT and industrial control systems. These new vulnerabilities at the edge are exposed, where sensitive tasks are performed without robust perimeter defenses. Disruptions of 5G infrastructure or edge computing nodes could impact supply chains, healthcare, or consumer applications. To thoroughly manage risk, from firmware updates to identity checks at the edge, the cyber security trends and challenges around 5G need to be observed.

6. Insider Threats Amplified by Hybrid Work

Insiders, such as a mix of remote staff, contractors, and distributed teams, are responsible for raising severe threats. Though employees may not intend to, when they misconfigure sharing links for cloud-based collaboration tools, they can expose sensitive files. Disgruntled staff could steal intellectual property in the meantime. The latest cyber security trends in workforce security are tools that combine behavioral analysis and data loss prevention to mitigate insider-driven compromises.

7. Supply Chain Attacks

Attackers target vendors or third-party software and thereby compromise multiple downstream organizations at once. The ripple effect of compromised updates is brought to light by high-profile events, such as SolarWinds. This continues to be a top cyber security trend, forcing companies to thoroughly vet the security posture of their

suppliers. Increasingly standard are contract clauses demanding continuous compliance and real-time monitoring of partner connections.

8. Cloud Container Vulnerabilities

Agility comes with containers and microservices, but so do new attack avenues if misconfigurations or unpatched images remain. It can pivot to the main environment from a single infected container to exfiltrate data or inject malicious code. Embedding checks in DevOps pipelines is an essential practice ("shift-left" security). Container security is a front and center cyber security trend and challenge for 2025 as businesses speed up DevOps.

9. Social Engineering via Deepfakes

Scammers can convincingly impersonate executives or celebrities through sophisticated audio-video manipulation. Voice calls based on deepfakes can fool employees to transfer funds or disclose credentials. As video conferencing has become the norm of remote work, deepfake phishing is a potent threat. These forms of manipulated social engineering are combated with awareness training and advanced verification steps.

10. Convergence of IT and OT Security

Traditionally, Operational technology (OT) domains such as manufacturing or critical infrastructure remained air-gapped from IT networks. However, as data driven insight and OT get merged in the context of Industry 4.0, new vulnerabilities emerge. Integration of specialized solutions is required because attackers can disrupt production lines or override safety systems. The latest trend in cyber security is to monitor both IT and OT for end-to-end coverage from enterprise apps down to the factory floors.

11. The increasing importance of supply chain security

Supply chain security breaches are indeed on the rise, with attackers exploiting vulnerabilities in third-party vendors to infiltrate larger networks. Monitoring of these third-party relationships is often insufficient. Most companies do not know all the third parties that handle their data and personally identifiable information (PII) and almost all companies are connected to at least one third-party vendor that has experienced a breach. This lack of oversight poses significant risks, as supply chain attacks can have cascading effects across industries.

Unsurprisingly, even prominent organizations fall victim to attacks via their suppliers' vulnerabilities. In 2025, organizations will need to prioritize investing in solutions that can vet and monitor their supply chain. AI-driven and transparency-focused solutions can help identify vulnerabilities in even the most complex supply chains. Organizations should also examine SLAs to select suppliers that maintain strict security protocols themselves, thereby creating ripples of improved security further down the ecosystem.

References:

https://thehackernews.com/2024/12/top-10-cybersecurity-trends-to-expect.html
https://securityintelligence.com/articles/cybersecurity-trends-ibm-predictions-2025/
https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-trends/

Contact Information:

Computer Emergency Response Team of Mauritius (CERT-MU)
Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu