bugcrowd

2025 CYBERSECURITY PREDICTIONS

Peacetime cyber vs. wartime cyber

In 10 years, we'll likely look back on this season as a defining period. As global tensions escalate and cyber makes itself obvious as a theater of modern warfare, the operating assumptions of cyber defenders will change. The true value of solutions and strategies developed during a period of relative "peace" will be challenged.

Secure by Design, Secure by Default

Ground-up cyber resilience initiatives like Secure by Design and Secure by Default will gain traction with product vendors, especially as the increase in malicious activity pressures vendors to deliver clear evidence of good cyber hygiene to their customers.

Hardware and IOT back in the spotlight

As nation-state threat actors continue to build and maintain their operational relay boxes (ORBs) and as the IAB business model continues to proliferate, the targeting of hardware in the form of IoT and edge-access devices will increase pressure on vendors to fix vulnerabilities quickly and avoid their introduction in the first place.

Casey Ellis, Founder and Advisor

Vendor consolidation will increase

In 2025, security vendor consolidation will accelerate in earnest. The operational inefficiencies of a fragmented security stack are hurting under-resourced security teams. Consolidating vendors reduces complexity and improves overall risk posture.

The importance of supply chain security

Supply chain security will rise in prioritization and prominence in the upcoming year. The security ecosystem is only as strong as its weakest link, and vulnerabilities within the supply chain can create huge ripple effects.

Increased CISO involvement in AI safety and security

CISOs will own AI safety and security strategies in 2025. With the widespread adoption of AI systems, CISOs will be expected to defend and secure this new attack surface. CISOs must ensure that AI models are mapped out and that risks are mitigated properly.

Dave Gerry, Chief Executive Officer

AI security liability and accountability will be in question

Organizations will continue to focus on securing all forms of AI for security vulnerabilities, bias, and data privacy. However, as organizations evolve, develop, and roll out agentic AI for core business processes (meaning that AI can make and act on its own informed business decisions autonomously), we'll see more liability and accountability events publicly surface when "bad AI" calls are made.

Third-party risk management (TPRM) processes need to be more robust

Threat actors (and hackers) will continue to focus on entry vectors via supply chain avenues. In turn, security and third-party assurance teams will need to show improvements and an increased vigilance in ongoing assurance testing methods to get deeper insights into supply chain "health." With suppliers also now leveraging AI, TPRM processes themselves will require uplift to assess this area more deeply. This will be crucial for organizations to keep up with supply chain attacks.

Investment budgets will decrease in "security mature" organizations for generic cyber asks

New security investment uplift budgets will start tapering off from previous years for pure-play control or capability asks. Accountability spotlights will shine higher on CISOs for ROI expectations to do more with what you have and consolidate security product sets. For any new investment requests, justification needs now be strongly tied to compliance, business revenue, or customer enablement objectives.

Nick McKenzie, Chief Information and Security Officer

Integration of AI with human expertise in pen testing approaches

While AI will handle routine and large-scale vulnerability scanning, human expertise will remain crucial for interpreting results and identifying nuanced or context-specific security issues. A collaborative approach will emerge where AI handles data analysis, and human pentesters focus on strategic thinking and creative attack vectors. This synergy will enhance the overall effectiveness of pen testing efforts.

Proliferation of deepfake technology-powered social engineering attacks

Criminals will harness advanced deepfake technology to create highly convincing fake audio and video messages from trusted individuals or organizations. These deepfakes will be used in spear-phishing campaigns and fraud schemes, making it increasingly difficult to distinguish genuine communications from malicious ones. This will lead to a surge in investment in deepfake detection technologies and stricter verification protocols.

Rise of continuous red team as a service offering

As organizations look to engage in continuous exposure management, ongoing or continual simulated attacks will become increasingly important to provide real-time feedback to organizations on evolving threat actor TTPs.

Julian Brownlow Davies, VP of Advanced Services

Securing LLMs will be the priority in 2025

"By 2025, bug bounty programs will focus heavily on securing LLMs and other AI-driven technologies as they become prime targets for attacks. Issues like prompt injection, data poisoning, and adversarial exploits will be at the forefront. At the same time, ethical hackers will use LLMs to speed up their recon and discovery processes, creating both new opportunities and new challenges."

Hx01, Hacker

Increased automated security outcomes

"I believe 2025 is going to be the takeoff year for automated cybersecurity outcomes. And by that, I mean they will manifest as actual products that work. AI-based Tier 1 analyst work has been pursued but hasn't been high-quality enough to be used in production. Hackbots exist and find some bugs, but they still aren't being deployed widely. I expect security vulnerabilities found by LLMs in code review to increase now that token cost has dropped significantly."

rez0, Hacker

RFID hacking will expand across all parts of the system

"I predict that RFID hacking will expand from purely hacking RFIDs to hacking all parts of a system especially with multiple backend tech options, like different radio-based technologies such as LoRa, Zigbee, Bluetooth, and Wi-Fi. From there, it will target APIs. The RFID end will possibly be a starting point of a kill chain, like what we saw with the latest Tesla TPMS hack. I also predict that RFID manufacturers will start evaluating their products from a hacker perspective to get a second opinion about their system and check if it is configured correctly."

Iceman, Hacker

More data leaks and phishing will occur as a result of AI

"All of the companies that rapidly integrated AI into their products will find themselves dealing with an unruly insider that will do anything, if asked nicely enough. I predict we'll see more incidents caused by a lack of/weak controls that result in privileged data leaking. AI and LLM technology becoming increasingly available and user-friendly will also result in the higher quantity and quality of phishing and vishing campaigns. Social engineering attempts will stray further away from traditional vectors like phone and email to social media platforms and communication platforms (like Slack and Discord)."

bl3ep, Hacker

AI will increase the importance and impact of ethical hacking

"2025 is shaping up to be a pivotal year for cybersecurity, fueled by advancements in AI and a growing recognition of ethical hacking. AI-driven exploits will become more sophisticated, but so too will AI tools aiding ethical hackers in vulnerability detection and remediation. The role of ethical hacking has never been more critical, and 2025 might just solidify it as a cornerstone of modern cybersecurity."

tess, Hacker