Artificial Intelligence is Not Just Changing Cybersecurity—It's Redefining It

Artificial intelligence is not just changing cybersecurity—it's redefining it. At the 2025 RSA Conference in San Francisco, where more than 40,000 cybersecurity and technology professionals convened, one theme stood out: AI is rapidly reshaping the cybersecurity landscape, bringing both unprecedented opportunities and significant challenges for both leaders and organizations.

Discussions about the emerging role of agentic AI revealed how deeply AI is embedded in the future of cyber operations. As AI quickly advances cyber threats, organizations seem to be taking a more cautious approach, balancing the benefits and risks of the new technology while trying to keep pace with attackers' increasing sophistication.

In turn, the cybersecurity market will benefit from two modes of growth: CISOs and cyber-risk professionals are embracing next-generation, AI-enabled security technologies. In addition, many large enterprises are still grappling with the basics—improving foundational areas such as IT asset management, vulnerability, and identity and access management. They will need to ramp up their efforts. Here are the three ways AI is impacting cybersecurity—and what organizations need to know to stay ahead.

1. AI is Changing the Threat Landscape—Fast

AI is accelerating the speed of cyberattacks, with breakout times now often under an hour. The ability of hackers to use AI tools—from creating convincing phishing emails, fake websites, and even deepfake videos to injecting malicious prompts or code—allows cybercriminals to craft personalized, realistic messages and methods that bypass traditional detection mechanisms. They can do so on an unprecedented scale.

Cybersecurity

In order to drive your digital transformation, your organization will need to build core capabilities that impact talent, infrastructure, and organization across the company.

Malicious actors can also weaponize and poison AI models used by companies, which raises concerns on model accuracy and outcomes. A common theme was the importance of Retrieval Augmented Generation (RAG)-based applications. That is, securing RAG workflows to mitigate risks in data retrieval, and ensuring the correct information is being used to build systems.

AI also enables attackers to become more productive and refine their strategies in real time. For example, machine learning algorithms can analyze an organization's defenses and adapt attack methods to exploit vulnerabilities. Social engineering tactics, such as impersonation and spear phishing, have become more effective, making it increasingly difficult for organizations to identify and prevent these threats. Organizations need to adopt advanced defenses to counter these AI-driven attacks.

2. AI is Powering Cybersecurity Defense

There's been a 1200% surge in phishing attacks since the rise of gen AI in late 2022.

While AI is a powerful tool for attackers, it is also a game-changer for cybersecurity defense. Organizations are leveraging AI to reduce their mean time to detect, respond, and recover and stay ahead of advanced attackers. Defensive AI systems can analyze vast amounts of data in real time, providing context across silos, identifying anomalies and potential breaches before they escalate. For example, AI can detect unusual login patterns, reverse-engineer malware, flag suspicious network activity, and even predict potential vulnerabilities based on historical data.

AI-driven automation is also transforming how organizations allocate their cybersecurity resources. By automating lower-risk tasks with AI agents, such as routine system monitoring and compliance checks, organizations can free up their teams to focus on high-priority threats. Targeted automation not only improves efficiency but also enhances overall risk management.

In parallel, agentic AI is expected to accelerate Security Operations Center automation, where AI agents could soon work alongside humans in a semi-autonomous manner to identify, think through, and dynamically execute tasks such as alert triage, investigation, response actions, or threat research. Additionally, AI-powered tools are being used to combat ransomware, one of the most pervasive threats facing businesses today.

3. AI Integration in Cybersecurity Solutions

The integration of AI into cybersecurity products is revolutionizing how organizations protect their systems and data. More than 90 percent of AI capabilities in cybersecurity are expected to come from third-party providers, making it easier for companies to adopt cutting-edge solutions as they upgrade their existing security stack. AI is being embedded into tools such as security posture management, Zero Trust capabilities, SASE, and Identity. Incorporating AI into existing cybersecurity products will support users to be more comfortable with the shift in technology.

Turning AI From a Risk Into an Ally

For many organizations, AI enablement is contingent upon continued progress in the fundamentals: knowing the who, what, where, and when of the enterprise technology estate at all times. These complexities are very real—multi-cloud, a heterogeneous network topography, frequent M&A, and non-human identities—just to name a few. Having knowledge and control of the estate is a precondition to enabling an AI security ecosystem. Without it, security AI will lack a mission by which to protect the estate.

Organizations who are vigilant about getting the underlying fundamentals of AI right can transform it from a potential risk into a powerful ally in the fight against cybercrime.