Q4 2025 Cybersecurity Update

Cybersecurity News/Insight

- The International Data Corporation projects cybersecurity spending to reach $377 billion by 2028.[1]The cost of cybercrimes for the world economy is expected to reach $10.5 trillion for the year 2025[2] with the average cost of a data breach at $4.4 million, a 9% y/y reduction driven by faster identification and containment.[3]
- In December 2025, the Cybersecurity and Infrastructure Security Agency (CISA) released its revised cross-sector cybersecurity performance goals, offering organizations a more robust framework for integrating cybersecurity into daily operations. It incorporates three years of operational insights, and addresses emerging threats through data-driven, actionable guidance.[4] The agency issued a joint advisory with the FBI and other U.S. and global partners urging immediate action to defend critical infrastructure from pro-Russia hacktivist threats.[5] The advisory warns of organized threat actors seeking targets of opportunity across all critical infrastructure sectors.[6]
- In December 2025, the United States halted plans to impose sanctions on China's ministry of state security over a massive cyber spying campaign (a wide-ranging and years-long cyberespionage campaign tracked as Salt Typhoon) to avoid derailing a trade truce struck by both countries this year.[7]
- In November 2025, the United States, Australia and Britain announced coordinated sanctions against Russia-based web company Media Land, accusing it of supporting ransomware operations. Britain has accused Media Land of being one of the most significant operators of so-called bulletproof hosting services, which provide infrastructure for ransomware and phishing attacks.[8]
- In November 2025, Google shutdown the group behind the E-ZPass, USPS text scam. Google said it has disrupted the foreign cybercriminal group behind a text scam operation within 24 hours of filing its lawsuit.[9]
- OpenAI has warned its upcoming AI models could pose a "high" cybersecurity risk, as their capabilities advance rapidly. The company further added it's investing in strengthening models for defensive cybersecurity tasks and creating tools that enable defenders to more easily perform workflows such as auditing code and patching vulnerabilities.[10]

Cybersecurity – Notable Ransomware Attacks and Breaches in Q4 2025

- On November 22, the OnSolve CodeRED emergency alert system, provided by Crisis24 in the U.S., was disrupted due to a cyberattack, preventing it from sending emergency notifications. The CodeRED system is used for alerts triggered by public safety events such as floods, gas leaks, chemical spills, fires, missing persons, and bomb threats. Crisis24 did not issue a statement, but customers reported that cybercriminals had obtained personal data of OnSolve CodeRED users. Some of the affected local government agencies said they are transitioning to a new CodeRED platform after the vendor discontinued the legacy platform targeted by the hackers. The Inc Ransom group which was behind the OnSolve attack listed it on its leak website on November 22. The attackers claimed negotiations failed because the vendor was only willing to pay a $100,000 ransom.[11]

- On November 20, Italy's national railway operator, the FS Italiane Group fell victim to a cyberattack after a threat actor breached Almaviva, the organization's IT services provider. The hacker claimed to have stolen 2.3 terabytes (TB) of data that include confidential documents and sensitive company information, and later leaked it on a dark web forum.[12]
- On November 14, Pajemploi, the French social security service for parents and home-based childcare providers, detected a data breach potentially exposing the personal information of 1.2 million individuals. The incident impacted registered professional caregivers working for private employers, typically parents using the Pajemploi service, which is part of URSSAF - the French organization that collects social security contributions from employers and individuals. Pajemploi stated that the incident did not impact its operations. No ransomware group has claimed credit for the attack.[13]
- On November 5, the University of Pennsylvania confirmed that data had been stolen in a cyberattack. The hackers used compromised credentials in a social engineering attack to breach the systems. The attacker hacked an employee's PennKey SSO account that provided access to the university's Salesforce instance, Qlik analytics platform, SAP business intelligence system, and SharePoint files. They stole 1.71 GB of internal documents. The attackers also stole a Salesforce donor marketing database, containing 1.2 million records with various donor information. In a post on a hacking forum, the attackers stated they are not currently leaking the data records but may do so within a month or two.[14]
- On October 27, Swedish state-owned power grid operator Svenska kraftnät confirmed that a data breach occurred following a cyberattack. The attack did not affect the country's power supply. The data breach was disclosed after the Everest ransomware group added Svenska to its Tor-based leak site and claimed to have stolen 280 GB of data.[15]
- On October 23, Freedom Mobile, the fourth-largest wireless carrier in Canada, detected a data breach. The attackers hacked into its customer account management platform and stole personal information of an undisclosed number of customers. Company officials stated that the incident was not a ransomware attack and did not affect the network and operations.[16]
- On October 19, Japanese retail company Muji suspended online sales in Japan due to a logistic outage caused by a ransomware attack on its delivery partner, Askul. All retail services were affected, including browsing or purchasing on online stores, viewing order histories via the Muji app, and displaying certain web content. Askul later confirmed that the attack caused significant disruptions to orders and shipping and resulted in 700,00 customer records being compromised. The RansomHouse ransomware group took credit for the attack and claimed to have stolen 1 TB of data which was leaked on November 10 and December 2, indicating the ransom was not paid.[17,18]
- On October 15, U.S.-based fencing and pet solutions provider Jewett-Cameron Company (Nasdaq: JCTC) reported a cyberattack. Following the attack, the company was unable to access several business applications related to operations and corporate functions. The company claimed IT related and financial information was exfiltrated but has yet to verify if employee's personal information was stolen. The identity of the attackers was not known, but they threatened to leak the stolen information if the ransom was not paid.[19]
- On October 14, Spanish fashion retailer MANGO notified customers of a data breach after its marketing vendor was compromised, exposing their personal data. MANGO specified that last names, banking information, credit card data, IDs, passports, or account credentials were not compromised in the incident.[20]
- On October 3, a hacking group believed to be a splinter of the ShinyHunters/Scattered Spider/LAPSUS$ collective released millions of records allegedly stolen from Salesforce customers. The attackers posed

as Salesforce staff and persuaded employees to install a malicious imitation of Salesforce Data Loader, granting them access to sensitive customer data. They claimed to have stolen 1 billion records from 39 Salesforce customers and demanded ransom from both Salesforce and the affected companies. Salesforce refused to pay, stating the Salesforce platform itself was not compromised. The group started leaking personal data on their Tor-based site for six of the named victims: Albertsons, Engie Resources, Fujifilm, GAP, Qantas, and Vietnam Airlines.[21,22]

- On October 2, sports betting company DraftKings (Nasdaq: DKNG), notified an undisclosed number of customers that their accounts had been hacked in a recent wave of credential stuffing attacks. Credential stuffing involves attackers using automated tools to breach user accounts with stolen username/password pairs from other online services, a tactic that is especially effective against those who reuse credentials across multiple platforms. The company said the attackers did not access sensitive data like government-issued identification numbers, full financial account numbers, or bank account details.[23]
- On September 29, Asahi Group Holdings (TYO: 2502) revealed that a cyberattack impacted 1.9 million individuals, including customers and employees. At the time of the attack, the company was forced to suspend production and shipping operations. The Qilin ransomware claimed responsibility and alleged to have stolen 27 GB of personal data and published samples of the data on their leak website.[24]

New Products

- In November 2025, Cisco (NASDAQ: CSCO) introduced foundational multi-customer management capabilities within Cisco security cloud control, purpose-built for managed service providers (MSPs). The innovation streamlines operations, reduces costs, and accelerates time-to-value for MSPs to deliver advanced managed security services.[25]
- In November 2025, Broadcom (NASDAQ: AVGO) introduced Brocade X8 Directors and Brocade G820 56-port switch, the industry's first 128G Fiber Channel platforms designed for mission-critical workloads and enterprise AI applications. Brocade Gen 8 Fiber Channel safeguards storage for the quantum era and automates infrastructure management through embedded SAN AI technology.[26]
- In November 2025, Fortinet (NASDAQ: FTNT) rolled out a secure AI data center solution, an end-to-end framework purpose-built to protect AI infrastructures. It is designed to secure the full AI stack from data center infrastructure to applications and large language models. The solution claims to deliver advanced AI threat defenses with ultra-low latency and reduce power consumption on average by 69% compared to traditional approaches.[27]
- In October 2025, Palo Alto Networks (NASDAQ: PANW) launched Cortex AgentiX, a secure platform to build, deploy and govern the AI agent workforce. The product claims to deliver up to a 98% reduction in mean time to repair with 75% less manual work.[28]
- In November 2025, Gen Digital (NASDAQ: GEN) launched Scam Guardian and Scam Guardian Pro for mobile devices. Building on the desktop product, this mobile expansion brings AI-powered scam protection directly to people's smartphones and tablets.[29]

Cybersecurity – M&A and IPO Activity in Q4 2025

- On November 19, Palo Alto Networks (Nasdaq: PANW) announced that it agreed to acquire observability platform provider Chronosphere in a deal valued at $3.35 billion, to be paid in cash and replacement equity awards. Chronosphere's platform enables teams to "zero in on the data that's most useful" and provides insights into every layer of their stack - infrastructure, applications and business.

The combined solution will integrate Chronosphere's observability platform with Palo Alto's AgentiX to deploy AI agents on massive datasets monitored by Chronosphere's platform. These agents will detect performance issues, autonomously investigate the root cause, and close the loop with agentic remediation. Chronosphere reported annual recurring revenue (ARR) of more than $160 million as of the end of September 2025.[30]

- On December 2, ServiceNow (NYSE: NOW) announced an agreement to acquire identity security company Veza Security. The terms of the deal are undisclosed, though reports indicated negotiations valued the company at over $1 billion. Earlier this year, Veza Security raised $108 million in a Series D funding round that valued the company at $808 million. Veza has developed an identity security platform that provides non-human identity management, SaaS access security, identity security posture management, privileged access monitoring, data system access, governance and administration, and cloud access management capabilities.[31]
- On October 21, real-time event and risk detection solutions provider Dataminr announced plans to acquire threat intelligence firm ThreatConnect for $290 million in cash and equity. Dataminr has developed a platform that leverages AI to process public data signals in search of critical events and threats, both in the physical and cyber worlds. It targets events such as natural disasters, civil unrest, vulnerabilities, data leaks, and financial market-moving events. Earlier this year, Dataminr announced raising $85 million in a funding round that brought the total investment in the company to over $1 billion. ThreatConnect provides a platform designed to help security teams aggregate, analyze and act on cyber threat intelligence and its solutions are used by Nike, Wells Fargo, Wyndham Hotels, and government agencies among others in the U.S., U.K., and Australia. The acquisition will help combine Dataminr's data signals platform with ThreatConnect's deep internal data capabilities to create agentic AI-powered intelligence that is tailored to the needs of each customer.[32]
- On October 21, data portability and resilience solutions provider Veeam Software announced plans to acquire data security posture management (DSPM) company Securiti AI for $1.725 billion in cash and stock. Veeam provides backup, disaster recovery, and data management solutions covering virtual, physical, and cloud environments. Securiti AI provides data security and governance solutions, helping organizations comply with global privacy regulations, automate data security, and manage risks across multi-cloud and decentralized data environments. The acquisition will enable Veeam to eliminate the challenge of managing fragmented data across apps, clouds, SaaS, endpoints, and backups.[33]

Venture Capital and Private Equity Activity:

- On December 4, agentic cybersecurity firm 7 AI announced that it had raised $130 million in Series A funding, bringing the total funds raised to $166 million. The funding was led by Index Ventures, with participation from new investor Blackstone Innovations Investments. 7 AI's 'swarming agents' can categorize threat alerts (whether they are cloud, email, identity, or EDR threats) and then dispatch appropriate agents to respond.[34]
- On November 5, exposure management and security company Armis announced that it had raised $435 million in a pre-IPO funding round that values the company at $6.1 billion. The funding round was led by Growth Equity at Goldman Sachs Alternatives, with participation from CapitalG, Evolution Equity Partners, and others. The funding will be used for strategic acquisitions, product enhancements, and go-to-market initiatives. The company has reported an ARR of over $300 million and the mission is to reach $1 billion in ARR. Armis has developed solutions that enable enterprises to discover IT, OT and IoT assets in their environments. In addition to asset intelligence and visibility, the company's platform

provides protection, risk assessment, vulnerability prioritization, and remediation and compliance capabilities.[35]

- On October 31, PE firm Francisco Partners entered into a definitive agreement to acquire Apple device management and security firm Jamf (Nasdaq: JAMF) in a $2.2 billion deal. Jamf provides a platform designed to help organizations manage and secure all their Apple devices, simplifying app deployment, updates, and patching. Francisco Partners will acquire all the outstanding shares of Jamf common stock for $13.05 per share in an all-cash transaction, which represents a 50% premium over the stock's 90-day average price before September 11, 2025. The transaction is expected to close in the first quarter of 2026.[36]
- On October 23, U.S.-based Chainguard announced that it raised $280 million in a growth funding round from General Catalyst's Customer Value Fund (CVF). The company has raised $636 million in the last six months alone, and nearly $900 million in total. In April, Chainguard raised $365 million in a Series D round, valuing the company at $3.5 billion. The company provides solutions for securing the open-source supply chain and has created secure-by-default container images that are not plagued by known vulnerabilities, making it easier for developers to build secure software. The company provides more than 1,700 such images, including for AI applications.[37]
- On October 23, Sublime Security announced that it raised $150 million in a Series C funding round that was led by Georgian, with participation from Avenir, 01A, Index Ventures, IVP, Citi Ventures, and Slow Ventures. The total funds raised by the firm stand at $240 million. The company has developed an agentic email security platform that leverages AI agents to analyze messages in search of threats. The platform uses a distributed detection model that conducts intent and behavioral analysis, along with deep content inspection. The platform can also automate workflows.[38]

[1] https://www.ibm.com/think/topics/cybersecurity
[2] https://www.ibm.com/think/topics/cybersecurity
[3] https://www.ibm.com/reports/data-breach
[4] https://www.cisa.gov/news-events/news/cisa-unveils-enhanced-cross-sector-cybersecurity-performance-goals
[5] https://www.cisa.gov/news-events/news/cisa-fbi-and-us-and-global-partners-urge-immediate-action-defend-critical-infrastructure-pro-russia
[6] https://www.cisa.gov/news-events/news/cisa-fbi-and-us-and-global-partners-urge-immediate-action-defend-critical-infrastructure-pro-russia
[7] https://www.usnews.com/news/world/articles/2025-12-03/us-halted-plans-to-sanction-chinese-spy-agency-to-maintain-trade-truce-ft-says
[8] https://www.reuters.com/world/asia-pacific/us-uk-australia-announce-sanctions-against-russia-based-media-land-over-2025-11-19/
[9] https://www.cnbc.com/2025/11/13/google-text-scam-phishing-e-zpass-usps.html
[10] https://money.usnews.com/investing/news/articles/2025-12-10/openai-warns-new-models-pose-high-cybersecurity-risk
[11] https://www.securityweek.com/ransomware-attack-disrupts-local-emergency-alert-system-across-us/
[12] https://www.bleepingcomputer.com/news/security/hacker-claims-to-steal-23tb-data-from-italian-rail-group-almaviva/
[13] https://www.bleepingcomputer.com/news/security/french-agency-pajemploi-reports-data-breach-affecting-12m-people/
[14] https://www.bleepingcomputer.com/news/security/university-of-pennsylvania-confirms-data-stolen-in-cyberattack/
[15] https://www.securityweek.com/hackers-target-swedish-power-grid-operator/
[16] https://www.bleepingcomputer.com/news/security/freedom-mobile-discloses-data-breach-exposing-customer-data/
[17] https://www.bleepingcomputer.com/news/security/retail-giant-muji-halts-online-sales-after-ransomware-attack-on-supplier/
[18] https://www.securityweek.com/700000-records-compromised-in-askul-ransomware-attack/
[19] https://www.securityweek.com/fencing-and-pet-company-jewett-cameron-hit-by-ransomware/
[20] https://www.bleepingcomputer.com/news/security/clothing-giant-mango-discloses-data-breach-exposing-customer-info/
[21] https://www.salesforceben.com/hackers-leak-millions-of-salesforce-customer-records-after-failed-ransom-bid/
[22] https://www.crn.com/news/security/hacker-group-says-1-billion-records-stolen-from-salesforce-users?itc=refresh
[23] https://www.bleepingcomputer.com/news/security/draftkings-warns-of-account-breaches-in-credential-stuffing-attacks/
[24] https://www.bleepingcomputer.com/news/security/japanese-beer-giant-asahi-says-data-breach-hit-15-million-people/
[25] https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2025/m11/cisco-simplifies-security-for-managed-service-providers-accelerating-their-hybrid-mesh-firewall-deployments-and-business-growth.html
[26] https://www.broadcom.com/company/news/product-releases/63686
[27] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2025/fortinet-launches-secure-ai-data-center-solution-to-protect-models-data-and-infrastructure-at-scale
[28] https://www.paloaltonetworks.com/company/press/2025/palo-alto-networks-unveils-cortex-agentix-to-build--deploy-and-govern-the-agentic-workforce-of-the-future
[29] https://newsroom.gendigital.com/2025-11-12-Avast-Brings-AI-powered-Scam-Defense-to-Mobile
[30] https://www.securityweek.com/palo-alto-networks-to-acquire-observability-platform-chronosphere-in-3-35-billion-deal/
[31] https://www.securityweek.com/servicenow-to-acquire-identity-security-firm-veza-in-reported-1-billion-deal/
[32] https://www.securityweek.com/dataminr-to-acquire-threatconnect-for-290-million/
[33] https://www.securityweek.com/veeam-to-acquire-data-security-firm-securiti-ai-for-1-7-billion/
[34] https://www.securityweek.com/agentic-security-firm-7ai-raises-130-million/
[35] https://www.securityweek.com/armis-raises-435-million-in-pre-ipo-round-at-6-1-billion-valuation/
[36] https://www.securityweek.com/jamf-to-go-private-following-2-2-billion-acquisition-by-francisco-partners/
[37] https://www.securityweek.com/chainguard-raises-280-million-in-growth-funding/
[38] https://www.securityweek.com/sublime-security-raises-150-million-for-email-security-platform/