Q4 2024 Cyber Security Update

Cyber Security News/Insight

- Revenue in the cybersecurity market is expected to grow to $185.7 bn in 2024, with an annual growth rate of 11.0%[1]. The security services segment is expected to contribute $97.3 bn to total revenues with the rest driven from cyber solutions.[2] During the period 2024-2029, revenue is expected to show an annual growth rate of 7.9%, resulting in a total market size of $271.9 bn by 2029[3]. This growth is expected to be led by the cyber solutions segment with an estimated CAGR of 10.9% and a resultant market size of $148.3 bn[4] by 2029, followed by the security services segment at a lower rate of 4.9% and a resultant market size of $123.6 bn by 2029[5]. Region wise, the largest market for cybersecurity, the U.S. is expected to have a market size of $81.4 bn in 2024 and is expected to grow at a CAGR of 7.4% during the period 2024-2029 to a market size of $116.2 bn by 2029.[6]
- According to Statista, cybercrimes are expected to cost about $9.2 tn in 2024 and an average cost per data breach at $4.9 mn, with the health care industry having the highest cost per breach (about $10 mn).[7, 8] The average cost per breach in the U.S. stood at $9.5 mn, close to twice the global average.[9] Furthermore, the cost of cybercrime worldwide is expected to grow by 69.4% from 2024 to $15.6 tn in 2029.[10]
- A recent survey by CyberArk (Nasdaq: CYBR) reveals that 65% of office workers circumvent company security policies in the name of efficiency, pointing to a fundamental challenge in the tradeoff between security and productivity.[11]
- In October 2024, the Cybersecurity and Infrastructure Security Agency (CISA) released its first ever international strategic plan.[12] The plan focuses on how CISA will proactively engage international partners to strengthen the security and resilience of the nation's critical infrastructure. "In following this plan, CISA will improve coordination with our partners and strengthen international relationships to reduce risk to the globally interconnected and interdependent cyber and physical infrastructure that Americans rely on every day," said CISA Director Jen Easterly.[13]
- In December 2024, U.S. Federal Communications Commission (FCC) chairwoman Jessica Rosenworce proposed a rule for communications service providers to submit an annual certification attesting that they have a plan in place to protect against cyberattacks[14]. This proposal followed the efforts of an alleged China-backed group of hackers, dubbed "Salt Typhoon," to dig deep into American telecommunications companies to steal data, including from phone calls.[15]
- In December 2024, European Union enacted two new laws to bolster its cybersecurity defenses and coordination mechanisms. The two laws are the Cyber Solidarity Act and amendments to the Cybersecurity Act (CSA)[16]. These laws will focus on threat detection, incident response, and service certification.
- In December 2024, NATO chief Mark Rutte announced intentions for setting up better intelligence sharing and for improving the protection of critical infrastructure in the face of "hostile" acts of sabotage against allies by Russia and China.[17]

Cybersecurity – Notable Ransomware Attacks and Breaches in Q4 2024

- On December 11, Krispy Kreme confirmed a cyberattack that led to operational disruptions including its online ordering system. The company mentioned that the attack is likely to have a material impact on its business operations until the recovery efforts are completed. The company's cybersecurity insurance is expected to cover a portion of the costs of the incident.[18]
- On December 9, medical devices company Artivion revealed a ransomware attack caused disruption to its order and shipping processes. The attack occurred on November 21 and forced Artivion to take some of its systems offline. Artivion believes that the attack did not have a material impact and is not likely to affect its finances and results of operations.[19]
- On December 9, Deloitte issued a statement after ransomware group Brain Cipher listed Deloitte U.K. on its Tor-based website and claimed to have stolen 1 TB of data. Deloitte has stated that its systems were not impacted, and the affected systems belong to a client outside of its network.[20]
- On December 5, British telecom giant BT became a victim of the Black Basta ransomware group which claimed to have stolen 500 Gb of data including financial, corporate, and personal information. The ransomware group added the company to its Tor-based leak website and threatened to publish the data if the ransom was not paid.[21]
- On December 4, U.S. White House disclosed Chinese hackers Salt Typhoon breached at least eight U.S. telecommunications companies in a month-long effort to spy on the communications of top politicians. Affected companies include AT&T, Verizon, T-Mobile, and ISP Lumen Technologies. The White House also mentioned that the campaign had been underway for 1-2 years, impacted dozens of countries, and that telecom companies may not have fully booted the hackers out of their systems.[22,23,24]
- On December 2, two National Health Service (NHS) hospitals – Alder Hey Children's Hospital Trust, and Liverpool Heart and Chest Hospital NHS Foundation Trust –disclosed cyberattacks in the U.K. The Inc Ransom added Alder Hey to its Tor-based leak website, claiming to have stolen data that includes patient records, donor reports, and other information dating from 2018-2024. The hospital stated that the attack did not impact the availability of its services.[25]
- On November 25, U.S.-based energy sector contractor ENGlobal Corporation was a victim of cyberattack and took certain systems offline to contain the damage. The company stated that recovery efforts were ongoing but could not provide an estimate as to when full access to its systems would be restored. No ransomware group has claimed responsibility for the attack.[26]
- On November 21, U.S.-based Blue Yonder revealed that its managed services hosted environment were affected due to a ransomware attack. Blue Yonder is a supply chain management software provider with several big clients. Starbucks confirmed that the attack disrupted its internal systems for managing employee schedules and tracking work hours in North America and Canada. U.K. supermarket chain Morrisons also faced disruptions in their operations. A new ransomware gang named Termite took credit for the attack on its Tor-based website and claimed to have stolen 680 Gb of data from Blue Yonder.[27,28,29]
- On November 8, U.S.-based oilfield supplier Newpark Resources announced that a ransomware attack disrupted information systems and business applications. The attacker's details were not shared. The company reverted to downtime procedures which allowed it to continue manufacturing with field operations uninterrupted.[30]
- On October 31, U.K.-based vehicle tracking solutions provider Microlise confirmed that a cyberattack impacted tracking systems and panic alarms in the prison vans and courier vehicles of at least two operators, namely DHL and Serco. In the week of November 23, the company revealed theft of

corporate data from its systems. Later, SafePay ransomware group listed the company on its Tor-based leak website, claiming the theft of 1.2 TB of data.[31]

- On October 5, Japan-based Casio fell victim to a ransomware attack from the Underground ransomware gang. The attack resulted in system disruptions and impacted some of the firm's services. On October 10, the attackers added Casio to its dark web extortion portal, leaking troves of sensitive data including intellectual property allegedly stolen from the Japanese firm.[32]
- On October 1, U.S.-based UMC Health System was forced to divert some patients to other locations after a ransomware attack caused an IT outage and impacted its network. The identity of the attackers was unknown at the time of the attack.[33]

New Products

- Towards the end of September 2024, Cloudflare (Nasdaq: NET) announced a new product called Speed Brain to speed up how webpages load by up to 45%, available for free.[34] It aims to eliminate load times completely by predicting the next page a user will visit, and downloading a webpage to the browser cache before a user navigates to it. Furthermore, Cloudflare has announced that its threat intelligence team, Cloudforce One, will make its research public for the first time ever as part of a commitment to democratize access to critical threat insights.[35]
- In November 2024, CrowdStrike (Nasdaq: CRWD) launched its AI Red Team services to proactively identify and help mitigate vulnerabilities in AI systems, including large language models (LLMs), so organizations can drive secure AI innovation with confidence.[36]
- In October 2024, Fortinet (Nasdaq: FTNT) announced the general availability of Lacework FortiCNAPP, a single, unified AI-driven platform to secure everything from code to cloud all from a single vendor.[37] The new product offers additional benefits such as “automated remediation and blocking of active runtime threats, as well as enhanced visibility into FortiGuard Outbreak Alerts, which provide key information about new and emerging threats and the risk they pose within an organization’s environment”.[38]
- In October 2024, Palo Alto Networks (Nasdaq: PANW) introduced its new operational technology solutions to address growing cybersecurity threats to industrial operations.[39] The solutions include a fully integrated, risk-based guided virtual patching solution, the Prisma Access Browser with Privileged Remote Access, and a suite of ruggedized, ML-powered next-generation firewalls (NGFWs) built to withstand harsh industrial settings where traditional firewalls often cannot operate.[40]
- In October 2024, Cisco (Nasdaq: CSCO) introduced its new AI-fueled solutions to enhance employee connection and collaboration, which include Cisco Spatial Meetings, Ceiling Microphone Pro, new Cisco AI Assistant for Webex capabilities and more.[41] Cisco has also announced its flagship new Cisco 360 Partner Program which is expected to roll out in February 2026. It is designed to “accelerate the value partners bring to customers by better addressing their rapidly evolving and complex needs, modernizing infrastructure, powering AI workloads anywhere, and keeping customers’ organizations secure, resilient, and high-performing”.[42] Additionally Cisco has rolled out plug-and-play AI solutions, accelerating AI adoption for the enterprise.[43]

Inside NQCYBR™ Index Activity:

- On December 12, Fortinet (Nasdaq: FTNT) acquired Israeli collaboration and email security company Perception Point for a reported amount of $100 mn. Perception Point provides solutions for securing email, collaboration platforms, web browsers, and cloud storage applications, which will enable Fortinet to expand and enhance its offering. Perception Point is known to have raised $48 mn in funding, with the most recent investment amount disclosed in 2021, when it secured $28 mn in a Series B round.[44]
- On November 6, CrowdStrike (Nasdaq: CRWD) announced its intent to acquire Israeli SaaS security firm Adaptive Shield in a $214 mn deal. Adaptive Shield provides comprehensive SaaS security posture management, enabling organizations to gain full visibility into misconfigurations, human and non-human identities, and data exposures across over 150 applications. CrowdStrike plans to integrate Adaptive Shield technology into its Falcon platform and will provide customers with comprehensive identity protection across SaaS, on-premises Active Directory and cloud-based environments. The acquisition was funded by cash, with the transaction being closed on November 20, 2024. Adaptive Shield, which emerged from stealth in 2020, raised $44 mn in funding, including $10 mn in 2023.[45,46]
- On October 8, Cloudlfare announced the acquisition of Kivera, a cloud security, data protection and compliance platform company. The combination of Kivera and Cloudlfare One platform will put controls directly into the cloud deployment process, preventing security issues and risks before they occur. It extends their SASE portfolio to incorporate cloud app controls, empowering Cloudflare One customers with preventative security controls for all their cloud services. The acquisition will add several capabilities including one-click security, enforced cloud treatment, data exfiltration and a flexible DevOps model.

Outside NQCYBR Index Activity:

- On November 14, cyber risk management solutions provider Bitsight announced that it will acquire Israel-based threat intelligence firm Cybersixgill for $115 mn. Cybersixgill harvests threat intelligence from millions of sources on the clear, deep, and dark web, and enriches it using automation and artificial intelligence to deliver alerts on emerging threats, indicators of compromise, and risk exposure. Bitsight's asset mapping capabilities and Cybersixgill's real-time threat data will provide highly relevant insights in the context of each organization's unique digital landscape, in a single solution.[47]
- On October 28, Socure, a provider of digital identity verification and fraud solutions, announced a deal to acquire Effectiv for $136 mn. Founded in 2021, Effectiv provides an AI orchestration and decisions platform that enables businesses to tackle account takeover, identity theft, scams, and real-time payment fraud challenges. The deal was expected to close in November 2024.[48]
- On October 17, data security company Cyera acquired data loss prevention (DLP) startup Trail Security, based in Israel, for $162 mn in cash and stock. Cyera is integrating its Data Security Posture Management (DSPM) with Trail's AI-enhanced DLP technology, turning it into a unified data security platform. Trail had previously raised $35 mn in funding from Lightspeed Ventures, CRV, and Cyberstarts.[49]
- On October 4, credit data company Experian (LON: EXPN) agreed to buy Brazilian cyber security firm ClearSale (BVMF: CLSA3) in a $350 mn deal. Experian will pay 10.56 reais per share of ClearSale, a 23.5% premium over ClearSale's Oct 3 closing price. Experian, whose local subsidiary Serasa has a leading position in credit information in Brazil, said it is betting on the "highly complementary" deal to enhance its identity and fraud (ID&F) business in the country. ClearSale has an active base of 7,400

clients with $91.72 mn in net revenues last year. Experian plans to fund the deal using cash resources and the issuance of Brazilian Depositary Receipts. The deal is expected to close in H1 2025, subject to approval from Brazilian regulators.[50]

Venture Capital and Private Equity Activity:

- On November 25, U.S.-based Halcyon closed $100 mn in Series C funding from Evolution Equity Partners with participation from Bain Capital Ventures (BCV), SYN Ventures, Harmony Group, Corner Capital Management, Dropbox Ventures, ServiceNow Ventures, and existing investors. The latest funding brings the total amount raised to $190 mn, including a $50 mn Series A in April 2023 and a $40 mn Series B in December 2023. Halcyon is marketing a platform promising a multi-tiered approach that uses AI/ML engines to defeat ransomware.[51]
- On November 20, data security company Cyera announced that it raised $300 mn in Series D funding at a valuation of $3 bn, led by Accel and Sapphire Ventures, with participation from Sequoia, Redpoint, Coatue, and Georgian. The total funds raised since the firm was founded in 2021 stood at $760 mn. In April 2024, the firm raised $300 mn in Series C funding at less than half the current valuation. Cyera provides an agentless, cloud-native platform that enables organizations to continuously discover, classify and secure data across cloud, SaaS, data lake, and on-premises environments.[52]
- On October 21, Thoma Bravo-owned, U.K.-based Sophos announced plans to acquire SecureWorks (Nasdaq: SCWX) in an all-cash deal valued at $859 mn. Shareholders of SecureWorks will receive $8.50 per share, a 28% premium to its 90-day average price. Sophos plans to combine its managed detection and response (MDR) services with SecureWorks' Taegis XDR platform to tap into lucrative markets across small, mid-sized, and enterprise segments. SecureWorks brings business tooling for identity threat detection and response (ITDR), next-gen SIEM capabilities, operational technology security, and enhanced vulnerability risk prioritization to Sophos. The deal is expected to close in early 2025.[53]

[1] https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[2] https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[3] https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[4] https://www.statista.com/outlook/tmo/cybersecurity/cyber-solutions/worldwide
[5] https://www.statista.com/outlook/tmo/cybersecurity/security-services/worldwide
[6] https://www.statista.com/outlook/tmo/cybersecurity/united-states
[7] https://www.statista.com/statistics/387861/cost-data-breach-by-industry/
[8] https://www.statista.com/markets/424/topic/1065/cyber-crime-security/#overview
[9] https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/

[10] https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide
[11] https://www.forbes.com/sites/larsdaniel/2024/12/05/new-study-finds-65-of-employees-bypass-cybersecurity-measures/
[12] https://www.cisa.gov/news-events/news/cisa-releases-its-first-ever-international-strategic-plan
[13] https://www.cisa.gov/news-events/news/cisa-releases-its-first-ever-international-strategic-plan
[14] https://www.reuters.com/technology/cybersecurity/fcc-chair-proposes-cybersecurity-rules-response-chinas-salt-typhoon-telecom-hack-2024-12-05/
[15] https://www.reuters.com/technology/cybersecurity/fcc-chair-proposes-cybersecurity-rules-response-chinas-salt-typhoon-telecom-hack-2024-12-05/
[16] https://www.consilium.europa.eu/en/press/press-releases/2024/12/02/cybersecurity-package-council-adopts-new-laws-to-strengthen-cybersecurity-capacities-in-the-eu/
[17] https://www.reuters.com/world/nato-boost-efforts-counter-russian-chinese-sabotage-acts-2024-12-03/
[18] https://www.securityweek.com/no-doughnuts-today-cyberattack-puts-krispy-kreme-in-a-sticky-situation/
[19] https://www.securityweek.com/medical-device-maker-artivion-scrambling-to-restore-systems-after-ransomware-attack/
[20] https://www.securityweek.com/deloitte-responds-after-ransomware-groups-claims-data-theft/
[21] https://www.securityweek.com/bt-investigating-hack-after-ransomware-group-claims-theft-of-sensitive-data/
[22] https://www.nbcnews.com/tech/security/chinese-hackers-stole-americans-phone-data-8-telecoms-us-officials-say-rcna182942
[23] https://www.pcmag.com/news/chinas-salt-typhoon-hacked-at-least-8-us-telecommunications-firms
[24] https://therecord.media/eight-telcos-breached-salt-typhoon-nsc
[25] https://www.securityweek.com/two-uk-hospitals-hit-by-cyberattacks-one-postponed-procedures/
[26] https://www.securityweek.com/energy-sector-contractor-englobal-targeted-in-ransomware-attack/
[27] https://www.securityweek.com/starbucks-grocery-stores-hit-by-blue-yonder-ransomware-attack/
[28] https://www.computing.co.uk/news/2024/security/ransomware-attack-on-blue-yonder-disrupts-starbucks-sainsburys-morrisons
[29] https://www.securityweek.com/blue-yonder-probing-data-theft-claims-after-ransomware-gang-takes-credit-for-attack/
[30] https://www.securityweek.com/texas-oilfield-supplier-newpark-hit-by-ransomware/
[31] https://www.securityweek.com/microlise-confirms-data-breach-as-ransomware-group-steps-forward/
[32] https://www.bleepingcomputer.com/news/security/underground-ransomware-claims-attack-on-casio-leaks-stolen-data/
[33] https://www.bleepingcomputer.com/news/security/ransomware-attack-forces-umc-health-system-to-divert-some-patients/
[34] https://www.cloudflare.com/en-in/press-releases/2024/cloudflare-speed-brain-make-millions-of-web-pages-faster/
[35] https://www.cloudflare.com/en-in/press-releases/2024/cloudflare-introduces-threat-intel-team/
[36] https://www.crowdstrike.com/en-us/press-releases/crowdstrike-launches-ai-red-team-services-secure-ai-systems/
[37] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2024/fortinet-expands-cloud-native-security-offerings-with-introduction-of-lacework-forticnapp
[38] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2024/fortinet-expands-cloud-native-security-offerings-with-introduction-of-lacework-forticnapp
[39] https://www.paloaltonetworks.com/company/press/2024/new-ot-security-solutions-from-palo-alto-networks-address-growing-cybersecurity-threats-to-industrial-operations
[40] https://www.paloaltonetworks.com/company/press/2024/new-ot-security-solutions-from-palo-alto-networks-address-growing-cybersecurity-threats-to-industrial-operations
[41] https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m10/cisco-unveils-new-ai-innovations-to-amplify-the-employee-experience-and-future-proof-the-workplace.html
[42] https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m10/cisco-unveils-new-cisco-360-partner-program-to-accelerate-value-and-innovation-launching-in-2026.html
[43] https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m10/cisco-unveils-plug-and-play-ai-solutions-accelerating-ai-adoption-for-the-enterprise.html
[44] https://www.securityweek.com/fortinet-acquires-perception-point-reportedly-for-100-million/
[45] https://www.securityweek.com/crowdstrike-to-acquire-adaptive-shield-in-reported-300-million-deal/
[46] https://ir.crowdstrike.com/node/13831/html
[47] https://www.securityweek.com/bitsight-to-acquire-cybersixgill-for-115-million/
[48] https://www.securityweek.com/socure-acquires-risk-decisioning-company-effectiv-for-136m/
[49] https://www.securityweek.com/cyera-acquires-data-loss-prevention-firm-trail-security-for-162-million/
[50] https://www.reuters.com/markets/deals/experian-buy-brazils-clearsale-377-million-report-says-2024-10-04/
[51] https://www.securityweek.com/halcyon-raises-100-million-at-1-billion-valuation/
[52] https://www.securityweek.com/cyera-raises-300-million-at-3-billion-valuation/
[53] https://www.securityweek.com/sophos-to-acquire-secureworks-in-859-million-all-cash-deal/