Q1 2025 Cybersecurity Update

Cybersecurity News/Insight

- Revenue in the Cybersecurity market is expected to grow to $203.0 bn in 2025, with an annual growth rate of 9.3%[1]. The Cybersecurity market generates revenue from two key segments: Cyber Solutions and Security Services. Cyber Solutions are tailored products or services that meet organizations' specific cybersecurity needs. Security Services encompass various processes and services that help improve an organization's overall security against cyber threats like phishing, malware, and ransomware. Out of the total $203.0 bn revenues forecasted in 2025, the Security Services segment is expected to contribute $103.1 bn to total revenues.[2] During the period 2025-2029, total revenue is expected to show an annual growth rate of 7.6%, resulting in a total market size of $271.9 bn by 2029[3]. This growth is expected to be led by the Cyber Solution segment with an estimated CAGR of 10.4% and a resultant market size of $148.3 bn[4] by 2029, followed by the Security Services segment at a lower rate of 4.6% 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 $88.2 bn in 2025 and is expected to grow at a CAGR of 7.1% during the period 2025-2029 to a market size of $116.2 bn by 2029.[6]
- According to Statista, cybercrimes are expected to cost about $10.3 tn in 2025 and is expected to grow to $15.6 tn in 2029.[7] Manufacturing, finance, and insurance were the most affected industries by cyberattacks. Within cyberattacks, ransomware was the most frequently detected, accounting for around 70 percent of all incidents.[8] The manufacturing industry faced the highest number of ransomware attacks, making it the most targeted sector globally.[9]
- In March 2025, the Cybersecurity and Infrastructure Security agency (CISA) released 13 Industrial Control Systems (ICS) advisories. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.[10] Furthermore, in partnership with the Federal Bureau of Investigation (FBI) and multi-state information sharing and analysis center (MS-ISAC), it has released a joint cybersecurity advisory to tackle Medusa ransomware (a ransomware-as-a-service). This advisory provides tactics, techniques, and procedures (TTPs), indicators of compromise (IOCs), and detection methods associated with known Medusa ransomware activity. Medusa actors commonly use phishing campaigns and exploit unpatched software vulnerabilities to gain access to a system.[11]
- In March 2025, the White House instructed agencies to avoid firing cybersecurity staff. The United States federal Chief Information Officer said, “we believe cybersecurity is national security and we encourage department-level Chief Information Officers to consider this when reviewing their organization”.[12]
- In February 2025, 23 industry groups across Europe have urged the EU tech chief to adopt EU cybersecurity label for cloud services that favors big tech and aims to help governments and companies choose a secure and trusted vendor for their cloud computing needs. The call came amid signs that the European Commission may delay adopting or even cancel the proposal, which has gone through several changes since it was unveiled by EU cybersecurity agency ENISA in 2020.[13]
- In March 2025, Australian securities watch dog, Australian Securities and Investments Commission (ASIC), announced that it is taking legal actions against FIIG (a fixed-income broker), alleging failure to implement

adequate cybersecurity measures over a four-year period starting from 2019, which enabled a hacker to infiltrate its IT network and putting about 18,000 clients personal information at risk.[14]

- According to the World Economic Forum (WEF), the cyber threat landscape in 2025 will be shaped by increasingly sophisticated attacks, with ransomware, social engineering and AI-powered cybercrimes. According to WEF, the six key cybersecurity vulnerabilities anticipated by leaders in 2025 are: I. Supply chain concerns, II. Geopolitical tensions, III. AI adoption risks, IV. Generative AI and cybercrime, V. Regulatory challenges and VI. Cyber talent shortage.[15]

Cybersecurity – Notable Ransomware Attacks and Breaches in Q1 2025

- On March 7, U.S.-based retirement services firm Carruth Compliance Consulting revealed that it was targeted by cyber attackers. Several schools and thousands of individuals were impacted as Carruth provides administrative services to public school districts and non-profit organizations for retirement savings plans. The breach was first detected on Dec 21, 2024. A new ransomware group, Skira, claimed to have stolen 469 Gb of data in the attack which included sensitive information such as Social Security numbers, financial account information, medical billing information and other important data.[16]
- On March 5, India-based engineering firm Tata Technologies (NSE: TATATECH) was a victim of cyberattack after Hunters International ransomware group threatened to leak 1.4 TB of stolen data and added the company to its Tor-based leak website. The ransomware group threatened to make the data public if the ransom was not paid.[17]
- On February 24, in the biggest cryptocurrency heist ever, hackers targeted the cryptocurrency exchange Bybit and stole approximately 400,000 Ethereum worth about $1.5 bn. The incident took place when Ethereum was being transferred from one of its cold wallets (secure offline storage) to a warm wallet (online storage and used for more frequent transactions). The hackers manipulated the user interface, altered the underlying smart contract logic and thereby were able to take control of the cold wallet and transfer assets to an address they controlled.[18]
- On February 19, U.S-based media company Lee Enterprises (Nasdaq: LEE) revealed that a cyberattack on February 3, caused significant disruptions. The attack affected the distribution of products, billing, collections, vendor payments and delays in distribution of printed publications. The company expects a phased recovery over several weeks. They indicated that there was a financial impact, the full scope of which was to be determined. The Qilin ransomware group took credit for the attack and claimed to have stolen 350 Gb of data.[19,20]
- On February 14, Nippon Steel (TYO: 5401) suffered a cyberattack by BianLian ransomware group. The ransomware group posted the company's name on its dark leak website and claimed to have stolen 500 Gb of personal and official data from Nippon's U.S. division networks. Later the company's name went missing from the leak site suggesting that Nippon may have been in the process of paying the ransom demand.[21]
- On January 30, Taiwan-based printed circuit board manufacturer Unimicron Technology (TPE: 3037) was targeted by cyber attackers. On Feb 11, the Sarcoma ransomware group listed the company on its Tor-based leak website threatening to leak 377 Gb of stolen data if the ransom was not paid.[22]
- On January 27, U.S.-based healthcare provider Frederick Health revealed that a ransomware disrupted their systems and delayed services. It was not known if any information was stolen. The identity of the attacker was not known either.[23]
- On January 26, New York Blood Center Enterprises (NYBCe) announced that a ransomware attack led to certain systems being taken offline. The identity of the attacker was not known. NYBCe, which

includes blood centers across the U.S., provides blood products to more than 400 hospitals in 17 states.[24]

- On January 10, Spain-based telecom company Telefonica (BME: TEF) confirmed that their internal ticketing system was breached after a stolen Telefónica Jira database was leaked on a hacking forum. The company revealed that their systems were breached using compromised employee credentials.[25]
- On January 8, U.S.-based BayMark Health Services notified patients that their personal information was stolen in a ransomware attack on the healthcare chain. The attack occurred between Sept 24 to Oct 14, 2024 and patient data including Social Security numbers, insurance information, and diagnosis and treatment information were stolen. Ransomhub ransomware group added BayMark to its Tor-based leak website in October and claimed to have stolen 1.5 Tb of data which they later made public.[26]
- On Jan 7, Sunflower Medical Group learnt that cyber attackers gained access to their systems from Dec 15, 2024 and stole vital personal and medical information of 220,000 individuals. The Rhysida ransomware group took credit and claimed to have stolen 3 Tb of data.[27]
- On January 7, PowerSchool, providing education software and services to more than 16,000 K12 schools and school districts in the U.S., Canada and in other countries, informed its customers that hackers stole vital information from their Student Information System (SIS) service. PowerSchool informed that a compromised credential was used to access the SIS. PowerSchool engaged with Canadian firm CyberSteward to negotiate with the attackers and ensure that the stolen data not be shared publicly, suggesting that they may have paid the ransom.[28]
- On January 2, prominent Singapore-based construction company Lian Beng Group was hit by ransomware by RansomHub ransomware group. The company has not released a statement on the extent of damage or its impact on the operations.[29]

New Products

- In March 2025, Cloudflare (Nasdaq: NET) announced that it is expanding end-to-end support for post-quantum cryptography to its Zero Trust Network Access solution. This enables organizations to securely route communications from web browsers to corporate web applications to gain immediate, end-to-end quantum-safe connectivity.[30]Furthermore, in February it announced a new, one-click solution for content creators and publishers to seamlessly preserve the digital history of an image–from how an image was created, and by whom, to edits and resizes–across the Cloudflare network.[31]
- In March 2025, Blackberry Limited (Nasdaq: BB) launched a functional safety platform to consolidate safety systems and AI workloads. The product is rolled with collaboration with Intel and NexCOBOT and delivers enhanced safety and efficiency in AI-powered robotics available on one platform.[32]Furthermore, it has announced the launch of its QNX General Embedded Development Platform (GEDP), designed to accelerate the development of high-performance, scalable, and secure embedded systems across various general embedded industries such as robotics, medical and industrial automation.[33]
- In January 2025, CrowdStrike Holdings (Nasdaq: CRWD) rolled out insider risk services to help organizations and Managed Security Service Providers (MSSPs) protect against insider risk, a growing cyberthreat that includes not only negligent or malicious employees but also outside sophisticated cybercriminal groups.[34]
- In March 2025, CyberArk Software (Nasdaq: CYBR) and Device Authority, in collaboration with Microsoft, launched a secure device authentication solution that strengthens and scales connected device authentication to enterprise applications with Zero Trust principles. It helps manufacturers reduce cyber risk

from connected devices in factory floors and edge environments with robust identity security, automated access management and device lifecycle protection.[35]

- In January 2025, Cisco Enterprise (Nasdaq: CSCO) launched its Cisco AI Defense solution to enable and safeguard AI transformation within enterprises. According to the company, it's purpose-built for enterprises to develop, deploy and secure AI applications with confidence.[36]

Cybersecurity – M&A and IPO Activity in Q1 2025

- On February 11, CyberArk Software (Nasdaq: CYBR) announced it acquired Identity Governance and Administration (IGA) vendor Zilla Security for $165 mn in cash, and $10 mn in performance-based earn-out. Zilla Security pitched AI-driven tools designed to automate labor-intensive processes such as user provisioning and compliance reviews — traditional pain points in legacy IGA systems. CyberArk plans to add these capabilities into its Identity Security Platform to market a single pane of glass for privilege management, lifecycle automation, and out-of-the-box integrations with popular SaaS and cloud applications.[37]
- On January 29, cybersecurity giant Tenable (Nasdaq: TENB) announced its intention to acquire exposure management company Vulcan Cyber for $150 mn, with $147 mn in cash and $3 mn in stock. Vulcan's solutions would improve Tenable's exposure management platform, including capabilities that will enhance customers' ability to consolidate exposure across their security stack, prioritize risks, and streamline remediation. The deal is expected to close in Q1 2025.[38]
- On February 11, security and compliance automation solutions provider Drata announced that they entered into a definitive agreement to acquire SafeBase in a $250 mn deal. SafeBase has created a trust center platform that automates security reviews, enabling customers to expedite security questionnaires with AI assistance. Together, they intend to enhance transparency and streamline self-serve security reviews, scale compliance and simplify audits, and enhance vendor risk management for organizations.[39]
- On January 28, U.S.-based endpoint management and security firm NinjaOne announced its intention to acquire Dropsuite for $252 mn. Australia-based Dropsuite specializes in cloud data backup, archiving, and recovery solutions designed to work with popular cloud services such as Microsoft 365 and Entra ID, Google Workspace and QuickBooks Online. The plan is to combine NinjaOne's automated endpoint management platform with Dropsuite's data protection suite. The deal is expected to close in H1 2025.[40]
- On January 13, blockchain analytics company Chainalysis announced that they acquired fraud detection startup Alterya for a reported amount of $150 mn. Chainalysis amasses troves of intelligence on crypto wallets to trace where money is moving while Alterya uses data on scammers to disrupt their transactions mid-route. Chainalysis believes Alterya's AI driven fraud models have substantial opportunities in the traditional market and help financial institutions, fintechs and crypto service providers prevent authorized push-payment (APP) fraud.[41,42]

Venture Capital and Private Equity Activity:

- On March 3, U.S.-based ransomware defense company Mimic announced that they raised $50 mn in Series A funding from Google Ventures (GV) and Menlo Ventures, with additional support from existing investors Ballistic Ventures, Shield Capital, Team8, and Wing Ventures. This funding comes less than a year after the company raised $27 mn in seed funding. The company's ransomware-focused platform can detect attacks early and stop them in real time before they can harm critical enterprise assets. The

company also announced a new capability that allows organizations to safely simulate the impact of ransomware on their environments, to improve their security posture, as necessary.[43]

- On February 17, Israel-based cybersecurity startup Dream announced raising $100 mn in Series B funding at $1.1 bn valuation. The latest round of funding led by Bain Capital Ventures, with additional support from Aleph, Group 11, Tau Capital, and Tru Arrow brings the total funds raised by the company to $155 mn. Dream has built an AI-powered solution that thinks both as an attacker and a defender, aiming to improve the cyber resilience of nations and their critical infrastructure. Dream's solution has been adopted by multiple governments and national cybersecurity entities, and the company reached $130 mn in annual sales last year.[44]

- On January 9, Darktrace, a portfolio company of investor Thoma Bravo, announced the proposed acquisition of the U.K.-based incident investigation and response firm Crado Security. Crado, which raised $31 mn in three funding rounds since 2020, has developed a cyber investigation and response solution that captures a screenshot of the data stored on a device and then conducts a forensic investigation in search of compromise or threat for multi-cloud, container, serverless, SaaS, and on-premises environments. Australian Financial Review reported that Darktrace is expected to pay around $50-$100 mn on completion of the deal, subject to regulatory approvals. The deal is expected to be completed in February 2025.[45,46]
- On December 18, Alphabet (Nasdaq: GOOG) spinoff SandboxAQ announced raising $300 mn at a valuation of $5.3 bn. The latest funding from a bunch of investors takes the total funding to over $800 mn. SandboxAQ develops several types of solutions that leverage AI and quantum technologies for cybersecurity, medical, materials science, chemistry, and navigation providing protection both against current attacks, as well as future quantum threats.[47,48]
- While Q4 revenue beat the consensus by $2.3 mn (1.7%), EPS missed consensus by $0.03. Sentiment was bearish due to the company's forward guidance and growth story.
- Q4 results indicated that top ten customers contributed 32% of revenue, down from 40% in Q4 2023, primarily due to revenue declines from few large customers. Enterprise customer count was 596, up 20 from Q3 2024. Enterprise customer average spend was $873,000, down 1% from $880,000 compared with Q3 2024 and Q4 2023. Remaining performance obligations (RPO) were $244 mn, up 4% from Q3 2024. LTM net retention rate (NRR) decreased to 102% vs. 105% in Q3 2024.
- Fiscal Q4 2024 revenue grew by a modest 2.0% y/y to $140.6 mn. On a q-o-q basis, revenue grew by 2.5%. EBIT stood a negative $33.9 mn vs. negative $42.6 mn in Q4 2023. Q4 2024 saw increased sales and marketing expenses, which are expected to drive a sales transformation into 2025. Net loss in Q4 was higher at $32.9 mn vs. net loss of $23.4 mn in Q4 2023. FCF was negative $11.1 mn vs. negative $16.0 mn in Q4 202.

- The company has hired a dedicated leader to strengthen its presence in the APAC region. Two dedicated leaders in North America will help in refining its strategy to better target different types of customers. Specifically, they are tailoring their approach for mid-market customers (smaller to medium-sized businesses) and enterprise customers (large businesses). The company has invested in compensation and incentives to support these growth initiatives through new customer acquisitions and cross-selling opportunities.
- Q1 2025 revenue was guided to be in the range of $136-$140 mn. Non-GAAP EBIT is expected to be in the range of negative $11-$7 mn. Non-GAAP EPS is expected in the range of a negative $0.09-$0.05. LTM NRR benchmark will remain flattish near term, followed by expansion in H2 2025. FY 2025 revenue

was guided to be in the range of $575-$585 mn. The company expects a net loss for FY 2025 with a non-GAAP EPS in the range of negative $0.15-$0.09.

[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/forecasts/1280009/cost-cybercrime-worldwide
[8] https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide
[9] https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide
[10] https://www.cisa.gov/news-events/alerts/2025/03/13/cisa-releases-thirteen-industrial-control-systems-advisories
[11] https://www.cisa.gov/news-events/alerts/2025/03/12/cisa-and-partners-release-cybersecurity-advisory-medusa-ransomware
[12] https://www.reuters.com/world/us/white-house-instructs-agencies-avoid-firing-cybersecurity-staff-email-says-2025-03-13/
[13] https://www.reuters.com/technology/cybersecurity/industry-groups-urge-quick-adoption-eu-cybersecurity-label-that-favours-big-tech-2025-02-28/
[14] https://www.reuters.com/technology/cybersecurity/australia-regulator-sues-fiig-securities-cybersecurity-failures-2025-03-12/
[15] https://www.weforum.org/stories/2025/02/biggest-cybersecurity-threats-2025/
[16] https://www.securityweek.com/many-schools-report-data-breach-after-retirement-services-firm-hit-by-ransomware/
[17] https://www.securityweek.com/ransomware-group-claims-attack-on-tata-technologies/
[18] https://www.securityweek.com/1-5-bn-bybit-heist-linked-to-north-korean-hackers/
[19] https://www.securityweek.com/lee-enterprises-newspaper-disruptions-caused-by-ransomware/
[20] https://www.securityweek.com/ransomware-group-takes-credit-for-lee-enterprises-attack/
[21] https://cybernews.com/news/nippon-steel-claimed-by-bianlian-ransomware-group/
[22] https://www.securityweek.com/circuit-board-maker-unimicron-targeted-in-ransomware-attack/
[23] https://www.securityweek.com/frederick-health-hit-by-ransomware-attack/
[24] https://www.securityweek.com/new-york-blood-bank-hit-by-ransomware/
[25] https://www.bleepingcomputer.com/news/security/telefonica-confirms-internal-ticketing-system-breach-after-data-leak/
[26] https://www.securityweek.com/major-addiction-treatment-firm-baymark-confirms-ransomware-attack-caused-data-breach/
[27] https://www.securityweek.com/560000-people-impacted-across-four-healthcare-data-breaches/
[28] https://www.securityweek.com/mns-impacted-by-powerschool-data-breach/
[29] https://cyberpress.org/qiant-lian-beng-ansomware/
[30] https://www.cloudflare.com/press-releases/2025/cloudflare-advances-industrys-first-cloud-native-quantum-safe-zero-trust/
[31] https://www.cloudflare.com/press-releases/2025/cloudflare-launches-one-click-content-credentials-to-track-image-authenticity/
[32] https://www.blackberry.com/us/en/company/newsroom/press-releases/2025/qnx-launches-functional-safety-platform-to-consolidate-safety-systems-and-ai-workloads
[33] https://www.blackberry.com/us/en/company/newsroom/press-releases/2025/qnx-unveils-general-embedded-development-platform-to-accelerate-developer-innovation
[34] https://www.msspalert.com/news/crowdstrike-unveils-insider-threat-services-for-mssps-organizations
[35] https://www.cyberark.com/press/cyberark-and-device-authority-in-collaboration-with-microsoft-deliver-secure-device-authentication-for-manufacturers/
[36] https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2025/m01/cisco-unveils-ai-defense-to-secure-the-ai-transformation-of-enterprises.html
[37] https://www.securityweek.com/cyberark-expands-identity-security-play-with-165m-acquisition-of-zilla-security/
[38] https://www.securityweek.com/tenable-to-acquire-vulcan-cyber-for-150-mn/
[39] https://www.securityweek.com/drata-to-acquire-safebase-in-250-mn-deal/
[40] https://www.securityweek.com/ninjaone-to-acquire-dropsuite-for-252-mn/
[41] https://www.coindesk.com/business/2025/01/13/chainalysis-buys-israeli-fraud-detection-startup-alterya-for-150-m
[42] https://www.fintechfutures.com/2025/01/chainalysis-acquires-ai-fraud-detection-solution-alterya/
[43] https://www.securityweek.com/mimic-raises-50-mn-to-stop-ransomware-attacks/
[44] https://www.securityweek.com/ex-nso-group-ceos-security-firm-dream-raises-100m-at-1-1b-valuation/
[45] https://www.securityweek.com/darktrace-to-acquire-incident-investigation-firm-cado-security/
[46] https://darktrace.com/news/darktrace-announces-proposed-acquisition-of-cado-security-a-cloud-investigation-and-response-specialist
[47] https://www.securityweek.com/sandboxaq-raises-300-mn-at-5-3-bn-valuation/
[48] https://www.sandboxaq.com/press/sandboxaq-announces-more-than-300-mn-of-funding-to-drive-next-era-of-ai