Q4 2023 Cyber Security Update

Cyber Security News/Insights

- During the period 2016-2022, the cybersecurity market grew at a compound annual growth rate (CAGR) of 12.5%, to a market size of $150.2 billion in 2022.[1] Cybersecurity revenue is expected to grow at an annual rate of 10.7% to $166.2 billion in 2023 with $88.0 billion coming from the security services segment and the rest from cyber solutions.[2] During the period 2023-2028, the market is estimated to grow at a compound annual growth rate (CAGR) of 10.5% to a market size of $273.6 billion in 2028, according to Statista. This growth is expected to be led by the cyber solution segment with an estimated CAGR of 15.2% and a resultant market size of $158.8 billion[3] in 2028, followed by the security services segment at a lower rate of 5.5% and a resultant market size of $114.7 billion in 2028.[4] Region wise, the largest market for cybersecurity, the U.S. is expected to have a market size of $71.8 billion in 2023, and is expected to grow at a CAGR of 9.7% during the period 2023-2028 to a market size of $113.8 billion by 2028.[5]
- According to Statista, cybercrimes are expected to cost about $8.2 trillion in 2023 with the cost expected to grow to $13.8 trillion in 2028.[6] The World Economic Forum's (WEF) Global risks report places cybersecurity in the top 10 global risks in the coming two- and ten-year periods. Power grids, water utilities and oil refineries are most vulnerable to attacks in cyberspace and pose a significant human risk.[7] In 2022, 40% of all nation-state attacks that were detected by Microsoft targeted critical infrastructure.[8]
- In 2023, cybersecurity spending growth came down nearly two-thirds from the spending growth seen in security budgets in 2022 (based on detailed budget data from 550 CISOs).[9] However, the cybersecurity's share of IT budgets continues to grow, reaching 11.6% in 2023 from 8.6% in 2020.[10]
- According to 2023, ISC2 Cybersecurity Workforce Study, the global cybersecurity workforce grew by 8.7% y/y to 5.5 million in 2023, however the shortfall between the number of workers needed and the available workforce grew at a higher pace, 12.6% y/y to 4.0 million.[11] Furthermore, the study cites cloud security as the most sought-after cybersecurity skill followed by zero-trust.[12]
- The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the UK National Cyber Security Centre (NCSC), along with partner agencies from 17 nations, have released Guidelines for Secure AI System Development.[13] They provide security considerations and risk mitigations for four stages of the AI development lifecycle: secure design, secure development, secure deployment, and secure operation and maintenance.[14] The Guidelines also urge AI systems developers to "take primary responsibility for the security of AI systems rather than to push responsibility down to system users".[15]
- Companies including Google and Amazon say they have fought off the world's biggest distributed denial of service (DDoS) attack, which began in August 2023 and was 7.5 times larger than the previous biggest attack.[16] "Any enterprise or individual that is serving an HTTP-based workload to the internet may be at risk from this attack," Google says.[17]
- The U.K. government's recent report states that cybersecurity risks are likely to increase because of generative AI, through "faster-paced, more effective and larger-scale cyber-intrusion via tailored phishing methods or replicating malware". But the report does not see hacking becoming fully automated by 2025.[18]

- Australia, in the wake of recent high-profile breaches, has announced a new wide-reaching cybersecurity plan with an objective of becoming a leader in the cybersecurity space by 2030. "The new strategy aims to shift the perception of cybersecurity from a technical issue to something all citizens and businesses can have an impact on".[19]
- According to a report prepared on behalf of Tenable, an exposure management company, in November 2023, APAC organizations could not prevent 41% of the cyberattacks on their business over the last two years. Furthermore, the report indicated that cybersecurity teams spent most of their time in addressing immediate threats and less time on proactive stances and struggling to identify the right threats to remediate.[20]

Cybersecurity – Notable Ransomware Attacks and Breaches in Q4 2023

- On Dec 1, office supply retail superstore Staples confirmed that it was a victim of a cyberattack that affected its online processing and delivering capabilities, as well as the company's communications channels and customer service lines.[21]
- On Nov 30, workforce analytics services provider ZeroedIn started reaching out to two million individuals informing them that their personal information was compromised in a cyberattack between Aug 7-8. Some of their affected clients included store chains Dollar Tree and Family Dollar. The stolen information contained names, dates of birth, and Social Security numbers.[22]
- On Nov 28, one of the world's largest automotive parts suppliers and a supplier to all the major automakers Yanfeng Automotive Interiors (Yanfeng) fell victim to the Qilin ransomware group. The attack forced the company to halt production at its North American plants the week of Nov 13, but full production had resumed by November 16. Qilin threatened to publish all the data if the ransom was not paid.[23]
- On Nov 27, U.S. based Ardent Hospitals announced that a ransomware attack disrupted its clinical and financial operations on Thanksgiving morning. Following the attack, Ardent and its affiliates rescheduled non-emergency procedures and diverted patients to other hospitals. The hospital is yet to confirm the extent of the damage and the amount of data leak.[24]
- On Nov 27, Iran-linked "Cyber Av3ngers" hackers targeted multiple organizations in the U.S. The Municipal Water Authority of Aliquippa, Pennsylvania was one of multiple victims breached by hackers who targeted a specific industrial control device because it is Israeli-made. The same group is said to have attacked four other utilities and an aquarium in the U.S. The programmable logic controller device made by Israel-based Unitronics, is used across a wide spectrum of industries including water and sewage-treatment utilities, electric companies, and oil and gas producers.[25,26,27]
- On Nov 22, car parts giant AutoZone (NYSE: AZO), which has over 7,000 stores across the Americas revealed that it had been attacked and informed 185,000 individuals of a compromise in their personal information. The data breach was caused by the MOVEit hack, and the data infiltration happened on Aug 15.[28]
- On Nov 16, Toyota Financial Services (TFS) confirmed that it detected unauthorized access to its systems in Europe and Africa. The Medusa ransomware gang demanded a payment of $8 million to delete the allegedly stolen data. TFS, a subsidiary of Toyota Motor Corporation, is a global entity with a presence in 90% of the markets where Toyota sells its cars, providing auto financing to its customers.[29]
- On Nov 14, Denmark's SektorCERT association revealed that 22 energy firms' systems were intruded by cybercriminals in a coordinated attack against Denmark's critical infrastructure in May 2023. The hackers exploited multiple vulnerabilities in Zyxel firewalls for initial access, executing code and gaining

complete control over the impacted systems. SektorCERT worked with the organizations that were impacted and secured the compromised networks immediately after identifying the attacks.[30]

- On Nov 13, U.S.-based healthcare delivery system McLaren Health Care revealed that their systems were breached between July 28 and Aug 22 and that the personal and medical information of nearly 2.2 million individuals was compromised. The organization was able to plug the breach but as a precautionary measure notified the individuals. The Alphv/BlackCat ransomware gang threatened to auction the stolen data.[31]
- On Nov 13, Australian shipping giant DP World was hit by a cyberattack that led to disruptions at the ports of Sydney, Melbourne, Fremantle, and Brisbane. Ships were able to unload their containers but the attack prevented freight from leaving the port.[32]
- On Nov 10, China's biggest bank, the Industrial and Commercial Bank of China Financial Services (SHA: 601398) announced a ransomware attack forcing it to disconnect the affected systems which caused minor disruptions to the U.S. treasury market. Its division in the U.S. manages trades and other services for financial institutions. Though the bank did not divulge any information, reports suggested the handiwork of LockBit gang was behind the attack.[33,34]
- On Nov 9, Japan Aviation Electronics (TYO: 6807) admitted to being a victim of a cyberattack on Nov 2, which caused some delay in receiving and sending mails. The company found no evidence of an information leak but the Alphv/BlackCat ransomware gang claims to have stolen about 150,000 documents from the company, including blueprints, contracts, confidential messages, and reports.[35]
- On Nov 7, Singapore's Marina Bay Sands luxury resort (owned by the U.S. casino and resort giant Las Vegas Sands) disclosed that 665,000 of its customers were impacted by a data breach on Oct 19 and 20. The type of data exposed in the incident can be used for targeted phishing attacks. Marina Bay Sands did not disclose the attacker's name, and no ransomware gang claimed credit for the attack.[36]
- On Nov 2, mortgage giant Mr. Cooper disclosed that a cyberattack on Oct 31 led to service disruptions. The company promptly shut down some of its systems which prevented customers from making online payments on their loans through the company's site. Mr. Cooper is one of the largest mortgage servicers in the U.S., with approximately 4.3 million customers.[37,38]
- On Oct 30, Boeing (NYSE: BA) informed the media that the LockBit ransomware gang infiltrated its distribution business stealing substantial amounts of data. Initially, the cybergang only made a mention of the attack on its leak site but two weeks post the attack published the stolen data on their site with 40 GB of data available for download, which suggested that the company refused to pay a ransom. Boeing reassured the public that the leaked data does not pose a threat to aircraft or flight safety.[39,40]
- On Oct 25, the cyberattack on the Philippines subsidiary of Yamaha Motor (TYO: 7272) resulted in employees' personal information being stolen. Yamaha Motor confirmed the attack a month later, on Nov 25. The INC Ransom gang has claimed responsibility for the cyberattack and has published a part of the stolen data on its leak site.[41]
- On Oct 23, Japanese electronics maker Casio (TYO: 6952) disclosed that the personal information of customers in 150 countries was exposed in a data breach and that the incident was discovered on Oct 11. The hackers gained access to a database in the development environment for ClassPad.net, an education web application that Casio manages and operates.[42]
- On Oct 21, American Family Insurance confirmed shutting down its IT systems resulting from a cyberattack. The nature of the attack is not clear, but signs indicate it was a ransomware attack. Customers were unable to pay bills or file claims online. Investigations did not detect any impact to critical business, customer data processing or storage systems.[43]

- On Oct 20, identity and access management tech firm Okta (NASDAQ: OKTA) revealed that hackers broke into its support case management system and stole sensitive data that can be used to impersonate validated users. Okta has taken measures to protect their customers, including the revocation of embedded session tokens.[44]
- On Oct 20, KwikTrip, a U.S. chain of over 800 convenience stores and gas stations, confirmed it was targeted by cybercriminals which disrupted its IT systems and has impacted its rewards program and support systems since Oct 8. Customer payment details were compromised due to the breach. The company has not yet revealed if any personal or confidential information was compromised in the incident.[45,46]
- On Oct 15 and Nov 22, healthcare solutions giant Henry Schein (NASDAQ: HSIC) revealed that it suffered a cyberattack twice at the hands of the BlackCat/ALPHV ransomware gang. The first attack took place on Oct 15 and the second attack took place in November which disrupted its manufacturing and distribution businesses, as well as its e-commerce platform. Alternative channels were made available to receive orders and then shipped to customers. After the first attack, the ransomware gang claimed to have stolen 35 terabytes (TB) of data, including payroll data and shareholder information. As disclosed by the company on Nov 22, the ransomware gang encrypted the company's systems as the ongoing negotiations with them had failed.[47,48,49]
- On Oct 11, Air Canada (TSE: AC) suffered a data breach when its IT system was compromised by the BianLian extortion group. The group claimed to have exfiltrated technical and operational data spanning from 2008 to 2023, including details about the company's technical and security challenges alongside other confidential data of employees and the company. After the incident, the airline was forced to lock all 1.7 million mobile app accounts to protect its customers' data.[50]
- On Oct 9, UK-based cable manufacturing giant Volex (LON: VLX) admitted to being targeted by cybercriminals. However, the company mentioned that apart from minor disruption to global production levels its sites remain operational, and it did not expect any material financial impact from the incident. No ransomware group had claimed responsibility for the attack.[51]
- On Oct 5, Sony Corp. (TYO: 6758) confirmed that it was a victim of cyberattacks in two separate incidents by cybercriminals. Sony identified unauthorized activity on a single server located in Japan. A new ransomware group named RansomedVC claimed responsibility and offered to sell the stolen data. In another incident in June, the Cl0p ransomware group exploited a zero-day vulnerability in Progress Software's MOVEit managed file transfer (MFT) software to gain access to the files of hundreds of organizations that had been using the product. In October, Sony informed that the ClOp attack affected 6,800 people including current and former employees of Sony Interactive Entertainment and their family members.[52]
- On Oct 2, budget hotel chain Motel One Group, which operates 90 hotels in 13 countries, confirmed being victim to a ransomware attack in which some customer information and credit card data was stolen. The AlphV/Black Cat ransomware gang claimed responsibility and said to have exfiltrated roughly 6TB of data from the company, including booking details for the past three years, customer contact information, and credit card data, along with internal Motel One documents, and threatened to publish the data if the ransom was not paid.[53]

New Products

- In November 2023, Trend Micro Inc. (NASDAQ: 4704) announced the addition of cloud risk management to its flagship cybersecurity platform. The new service "drives business value by enabling organizations to consolidate their cybersecurity efforts and achieve a complete view of cloud security risks across hybrid IT environments".[54] Additionally, Trend Micro introduced its new generative AI tool, Trend Companion, designed to empower security analysts by driving streamlined workflows and enhanced productivity.[55]
- Norton, a consumer cyber safety brand of Gen Digital Inc. (NASDAQ: GEN), announced Norton Small Business, "an all-in-one cybersecurity solution to help entrepreneurs and small business owners protect their financial futures"[56]. Furthermore, the company has introduced a new private email feature in Norton AntiTrack, which changes email addresses and removes hidden trackers to bolster online privacy.[57]
- During the period October-November 2023, Palo Alto Networks (NASDAQ: PANW) introduced a few industry-first products leveraging AI into their offerings: I. Strata Cloud Manager, an AI powered zero trust management and operations solution[58], II. Prisma Cloud's Darwin, a cloud security product with industry-first integrated code to cloud intelligence[59], and III. Cortex XSIAM (AI-driven security operations platform) enhancements to enable customers to add their own custom AI models on the XSIAM data lake in addition to already existing models.[60] In addition, the company has announced five new next-generation firewalls "to expand addressable use cases, from the most high-traffic networks to remote branches, including ones that require 5G connectivity and others that need to operate in the harshest operational technology (OT) environments".[61]
- In October 2023, Qualys Inc. (NASDAQ: QLYS) introduced its VMDR TruRisk, FixIT and ProtectIT capabilities in AWS Marketplace "priced and packaged for small-to-medium sized businesses (SMBs) and small-to-medium enterprises (SMEs)", given the backdrop of increasing cyber-attacks on small businesses (up to 43% of cyberattacks targeting small businesses).[62]
- In October 2023, CyberArk Software (NASDAQ: CYBR) announced new capabilities for securing access to cloud services and modern infrastructure for all users, based on the company's risk-based intelligent privilege controls. It includes enhancements to its existing CyberArk Secure Cloud Access solution.[63] Additionally, in November, the company expanded password-less authentication capabilities with new passkeys support.[64]

Cybersecurity – M&A and IPO Activity in Q4 2023

Inside NQCYBR Index Activity:

- On October 31, Palo Alto Networks (NASDAQ: PANW) announced its intent to acquire Dig Security, an Israeli cloud security startup specializing in data security posture management (DSPM). The emerging space addresses deep data-related risks in the cloud. Arora noted the move is to double down on data security for generative artificial intelligence (genAI) and Prisma Cloud.[65]
- On Nov 6, Palo Alto (NASDAQ: PANW) announced plans to acquire Talon Cyber Security in a $625 million deal. Talon, an Israeli startup, sells a secure browser to enterprise customers that helps deal with risks from unmanaged devices. The firm had earlier raised about $143 million in three funding rounds since 2021. Palo Alto plans to integrate Talon's browser technology with its Secure Access Service Edge (SASE) suite to secure all managed and unmanaged devices with complete zero-trust principles.[66,67]

Outside NQCYBR Index Activity:

- On Nov 6, Travelers (NYSE: TRV), one of the leading global insurance companies with $30 billion in revenues, agreed to acquire U.S.-based Corvus Insurance Holdings for $435 million. Corvus is a cyberinsurance managing general underwriter and uses artificial intelligence (AI) for data analysis, loss prediction and prevention, catering to wholesale brokers and large retail producers. The acquisition provides Travelers with access to sophisticated underwriting algorithms, advanced cyber vulnerability scanning, and digital connectivity to customers and distribution partners. The transaction will be funded from internal resources and is expected to close in Q1 2024 subject to regulatory approvals and customary closing conditions. Travelers does not anticipate any material near-term impact on earnings.[68]

Venture Capital and Private Equity Activity:

- On Oct 30, PE firm Thoma Bravo's Proofpoint, an enterprise security vendor, announced its intention to acquire email security specialist Tessian, a U.K.-based startup selling cloud email security software. The acquisition will add to Proofpoint's technology to tackle data loss, including misdirected email and data exfiltration caused by employee negligence. The terms of the deal were not disclosed, but Tessian raised $65 million in Series C funding in 2021, and $123 million in total from earlier fundings, giving it a valuation of $500 million.[69,70]

- On Oct 25, U.S. startup Censys in a Series C funding raised $75 million from Decibel Partners, GV, Greylock and Intel Capital, as well as new investors Ascension Ventures and Four Rivers Partners. The firm claims to have the most complete and accurate collection of global internet infrastructure data and provides technology to enrich the data to drive security decisions. Censys counts prominent organizations like Google, NATO, the Swiss Armed Forces, and the U.S. Department of Homeland Security among its customers.[71]

- On Oct 24, U.S.-based startup Adlumin raised $70 million in a Series B funding from venture capital firm SYN Ventures alongside First In Ventures, Washington Harbour Partners, and BankTech Ventures. The latest funding round brings the total funds raised to $83 million. Adlumin's security tooling, sold through one license and one platform, includes security information and event management (SIEM), vulnerability scanning, threat intelligence, user behavior analytics (UEBA), threat hunting including honeypots, automated incident response and forensics, darknet exposure monitoring, compliance reporting and monitoring. The startup's customers include smaller law firms, banks, other financial services firms, schools, manufacturers, and healthcare providers otherwise overlooked by cybersecurity vendors.[72]

- On Oct 23, Island, a U.S.-based enterprise web browser startup, received an investment of $100 million in Series C funding from Prysm Capital valuing the company at $1.5 billion. Existing investors Canapi Ventures, Insight Partners, Stripes, Sequoia, Cyberstarts and Georgian also increased their equity positions. The firm has received total funding of $325 million from investors since its launch in 2020. The firm's Chrome-based product promises protection against data exfiltration (including data copy, transfer, and screenshot capture), along with more advanced capabilities, such as multi-factor authentication insertion and smart network routing. Island said it has sold 2 million browsers to customers in all major verticals and segments, and has multiple customers ranking in the top 20 of the Fortune 100.[73]

- On Oct 10, a new venture called Gutsy, founded by the team that created Twistlock, announced it received a massive $51 million in seed funding from YL Ventures and Mayfield. Gutsy is working on software that uses process mining to generate data-driven insights into the intricate web of an

organization's teams, tools, and processes, highlighting their functions and results. Twistlock was sold to Palo Alto in 2019 for $410 million.[74]

[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/cyber-solutions/worldwide
[4] https://www.statista.com/outlook/tmo/cybersecurity/security-services/worldwide
[5] https://www.statista.com/outlook/tmo/cybersecurity/united-states
[6] https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide#:~:text=The%20global%20indicator%20%27Estimated%20Cost,U.S.%20dollars%20(%2B69.94%20percent).
[7] https://www.forbes.com/sites/forbesfinancecouncil/2023/12/05/turning-cyber-offense-into-defense-for-successful-cybersecurity-investing/?sh=2cfdaa72dfd0
[8] https://www.forbes.com/sites/forbesfinancecouncil/2023/12/05/turning-cyber-offense-into-defense-for-successful-cybersecurity-investing/?sh=2cfdaa72dfd0
[9] https://cdn.iansresearch.com/Files/Marketing/2023SurveyContent/IANS+ArticoSearch-2023SecurityBudgetBenchmarkSummaryReport.pdf
[10] https://www.forbes.com/sites/forbesfinancecouncil/2023/12/05/turning-cyber-offense-into-defense-for-successful-cybersecurity-investing/?sh=2cfdaa72dfd0
[11] https://ciosea.economictimes.indiatimes.com/news/security/58-cyber-professionals-say-targeting-key-skills-gaps-can-mitigate-worker-shortages-report/104929529
[12] https://ciosea.economictimes.indiatimes.com/news/security/58-cyber-professionals-say-targeting-key-skills-gaps-can-mitigate-worker-shortages-report/104929529
[13] https://www.dwt.com/-/media/files/blogs/privacy-and-security-blog/2023/12/guidelinesforsecureaisystemdevelopment.pdf?la=en&rev=d963e9dfbb8b49ddbd0d6d180012f9a9&hash=881D452F65CED6015181662E3612CB01
[14] https://www.jdsupra.com/legalnews/cisa-uk-ncsc-and-17-other-countries-8412587/
[15] https://www.dwt.com/-/media/files/blogs/privacy-and-security-blog/2023/12/guidelinesforsecureaisystemdevelopment.pdf?la=en&rev=d963e9dfbb8b49ddbd0d6d180012f9a9&hash=881D452F65CED6015181662E3612CB01
[16] https://www.weforum.org/agenda/2023/11/biggest-ddos-attack-cybersecurity-news-to-know-november-2023/
[17] https://www.weforum.org/agenda/2023/11/biggest-ddos-attack-cybersecurity-news-to-know-november-2023/
[18] https://www.weforum.org/agenda/2023/11/biggest-ddos-attack-cybersecurity-news-to-know-november-2023/
[19] https://www.weforum.org/agenda/2023/12/black-friday-phishing-attacks-and-other-cybersecurity-news-to-know-this-month/
[20] https://ciosea.economictimes.indiatimes.com/news/security/apac-organisations-cannot-prevent-4-out-of-10-cyberattacks-study/104913814
[21] https://www.securityweek.com/staples-confirms-cybersecurity-risk-disrupting-online-stores/
[22] https://www.securityweek.com/dollar-tree-impacted-by-zeroedin-data-breach-affecting-2-million-individuals/
[23] https://www.bleepingcomputer.com/news/security/qilin-ransomware-claims-attack-on-automotive-giant-yanfeng/
[24] https://www.securityweek.com/ardent-hospitals-diverting-patients-following-ransomware-attack/
[25] https://www.securityweek.com/breaches-by-iran-affiliated-hackers-spanned-multiple-u-s-states-federal-agencies-say/
[26] https://www.securityweek.com/hackers-hijack-industrial-control-system-at-us-water-utility/
[27] https://www.securityweek.com/congressmen-ask-doj-to-investigate-water-utility-hack-warning-it-could-happen-anywhere/
[28] https://www.securityweek.com/185000-individuals-impacted-by-moveit-hack-at-car-parts-giant-autozone/
[29] https://www.bleepingcomputer.com/news/security/toyota-confirms-breach-after-medusa-ransomware-threatens-to-leak-data/#google_vignette
[30] https://www.securityweek.com/22-energy-firms-hacked-in-largest-coordinated-attack-on-denmarks-critical-infrastructure/
[31] https://www.securityweek.com/2-2-million-impacted-by-data-breach-at-mclaren-health-care/
[32] https://www.securityweek.com/operations-at-major-australian-ports-significantly-disrupted-by-cyberattack/

[33] https://www.securityweek.com/ransomware-attack-on-chinas-biggest-bank-disrupts-treasury-market-trades-reports-say/
[34] https://www.securityweek.com/yellen-says-ransomware-attack-on-chinas-biggest-bank-minimally-disrupted-treasury-market-trades/
[35] https://www.securityweek.com/japan-aviation-electronics-targeted-in-ransomware-attack/
[36] https://www.securityweek.com/marina-bay-sands-discloses-data-breach-impacting-665k-customers/
[37] https://www.securityweek.com/mortgage-giant-mr-cooper-shuts-down-systems-following-cyberattack/
[38] https://www.securityweek.com/mr-cooper-says-customer-data-compromised-in-cyberattack/
[39] https://www.securityweek.com/ransomware-group-leaks-files-allegedly-stolen-from-boeing/
[40] https://www.securityweek.com/boeing-investigating-ransomware-attack-claims/
[41] https://www.securityweek.com/yamaha-motor-confirms-data-breach-following-ransomware-attack/
[42] https://www.securityweek.com/casio-says-personal-information-accessed-in-web-application-server-hack/
[43] https://www.bleepingcomputer.com/news/security/american-family-insurance-confirms-cyberattack-is-behind-it-outages/
[44] https://www.securityweek.com/okta-support-system-hacked-sensitive-customer-data-stolen/
[45] https://www.bleepingcomputer.com/news/security/kwiktrip-all-but-says-it-outage-was-caused-by-a-cyberattack/
[46] https://www.bleepingcomputer.com/news/security/kwik-trip-finally-confirms-cyberattack-was-behind-ongoing-outage/
[47] https://www.securityweek.com/operations-of-healthcare-solutions-giant-henry-schein-disrupted-by-cyberattack/
[48] https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-breach-of-healthcare-giant-henry-schein/
[49] https://www.bleepingcomputer.com/news/security/healthcare-giant-henry-schein-hit-twice-by-blackcat-ransomware/
[50] https://www.bleepingcomputer.com/news/security/bianlian-extortion-group-claims-recent-air-canada-breach/
[51] https://www.securityweek.com/cable-giant-volex-targeted-in-cyberattack/
[52] https://www.securityweek.com/sony-confirms-data-stolen-in-two-recent-hacker-attacks/
[53] https://www.securityweek.com/motel-one-discloses-ransomware-attack-impacting-customer-data/
[54] https://newsroom.trendmicro.com/2023-11-28-Trend-Micro-First-to-Integrate-Cloud-Risk-Management-and-XDR-Across-Customers-Entire-Attack-Surface
[55] https://newsroom.trendmicro.com/2023-11-27-Trend-Micro-First-to-Market-with-AI-powered-Cybersecurity-Assistant-for-Security-Teams
[56] https://newsroom.gendigital.com/2023-09-27-Norton-Introduces-New-Small-Business-Solution-with-24-7-Triple-Lock-Cybersecurity-for-Small-Teams
[57] https://newsroom.gendigital.com/2023-10-19-Norton-Boosts-Security-and-Privacy-with-Enhanced-Password-Manager-and-AntiTrack
[58] https://www.paloaltonetworks.com/company/press/2023/palo-alto-networks-launches-strata-cloud-manager--industry-s-first-ai-powered-zero-trust-management-and-operations-solution
[59] https://www.paloaltonetworks.com/company/press/2023/palo-alto-networks-revolutionizes-cloud-security-with-industry-first-integrated-code-to-cloud-intelligence
[60] https://www.paloaltonetworks.com/company/press/2023/palo-alto-networks-adds--bring-your-own-ai--capability-to-cortex-xsiam-ai-driven-security-operations-platform
[61] https://www.paloaltonetworks.com/company/press/2023/palo-alto-networks-launches-strata-cloud-manager--industry-s-first-ai-powered-zero-trust-management-and-operations-solution
[62] https://investor.qualys.com/news-releases/news-release-details/qualys-announces-trurisk-fixit-and-protectit-packages-aws
[63] https://www.cyberark.com/press/cyberark-launches-new-capabilities-for-securing-access-to-cloud-workloads-and-services-as-part-of-its-identity-security-platform/
[64] https://www.cyberark.com/press/cyberark-elevates-passwordless-experience-with-new-passkeys-authentication/

[65] https://www.sdxcentral.com/articles/news/palo-alto-networks-sustains-1b-ma-with-twin-acquisitions/2023/11/
[66] https://www.securityweek.com/palo-alto-to-acquire-talon-intensifying-competition-in-cloud-data-security/
[67] https://cxotoday.com/news-analysis/palo-alto-networks-buys-talon-for-600mn/#:~:text=Having%20stayed%20off%20the%20acquisition,giant%20around%20a%20billion%20dollars.
[68] https://www.securityweek.com/travelers-to-acquire-cyberinsurance-firm-corvus-for-435-million/
[69] https://www.securityweek.com/proofpoint-to-acquire-tessian-for-ai-powered-email-security-tech/
[70] https://www.securityweek.com/email-security-firm-tessian-raises-65-million-500-million-valuation/
[71] https://www.securityweek.com/censys-banks-75m-for-attack-surface-management-technology/
[72] https://www.securityweek.com/adlumin-snags-70m-to-boost-security-for-mid-market-firms/
[73] https://www.securityweek.com/enterprise-browser-startup-island-banks-100m-in-funding/
[74] https://www.securityweek.com/twistlock-founders-score-whopping-51m-seed-funding-for-gutsy/