Q3 2023 Cyber Security Update

Cyber Security News/Insight

- 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] A survey conducted in September 2023 by Allied Universal found that almost half of security chiefs at the world's biggest companies expect to increase their budgets significantly in the next year as they see economic and social unrest driving more cases of theft, fraud and the leaking of sensitive information, with North America being badly affected.[7]
- During the Billington cybersecurity summit held in September 2023, the Cybersecurity and Infrastructure Security Agency (CISA)'s director announced that the Cyber Incident Reporting for Critical Infrastructure Act is in its final stages and expects to be done by the end of this year or early 2024 at the latest[8]. The act signed in March 2022 requires critical infrastructure providers to report major cyber incidents and ransomware payments to the agency.
- The Biden administration has alleged that China inserted a code designed to disrupt U.S. military operations in the event of a conflict. It was essentially "a ticking time bomb" that could give China the power to interrupt or slow American military deployments or resupply operations by cutting off power, water, and communications to U.S. military bases[9]. Additionally, the Pentagon has "pledged to use offensive cyber operations to frustrate and disrupt foreign powers and criminals that threaten US interests" in a new military strategy document released in September 2023. It also warns of China's aims to dominate cyberspace[10]. Additionally, the US Department of Defense (DoD)'s 2023 cyber strategy's key focus is to boost the cyber capabilities of allies and partners, and to increase collective resilience against cyberattacks.[11]
- The U.K. government has warned about targeted cyberattacks against its national healthcare system which have the potential to cause large scale disruptions and could take years to recover. The risk assessment report, published in August 2023, stated that critical infrastructure, including healthcare, is susceptible to destructive hacks. Additionally, a targeted ransomware attack with quick infection capabilities can have an almost immediate impact on the U.K.'s National Health Service".[12]
- According to a Bloomberg report published in September 2023, China accused the U.S. of hacking Huawei servers beginning in 2009. Additionally, the Chinese ministry report says that the U.S. has led tens of thousands of attacks on Chinese targets.[13]

Cybersecurity – Notable Ransomware Attacks and Breaches in Q3 2023

- On Sept 14, Caesars Entertainment (NASDAQ: CZR), a large casino chain in the U.S. discovered a cyberattack on Sept 7 targeting its loyalty program database which stores the driver's license numbers and social security numbers for many customers. Bloomberg reported the attacker to be Scattered Spider, a cybergang affiliated to ALPHV/ BlackCat active since May 2022, which uses a combination of social engineering, multi-factor authentication (MFA) fatigue, and SMS credential phishing attacks to steal user credentials and breach targets' networks. According to Wall Street Journal, Caesars paid ~$15 million of the $30 million ransom demanded. However, MGM insider @LasVegasLocally posted on X that Caesars paid the $30 million ransom demand.[14,15,16]
- On Sept 10, a cyberattack at MGM Resorts (NYSE: MGM) forced the entity to shut down some systems including its main website, online reservations, digital hotel room keys and in-casino services, like ATMs, slot machines, and credit card machines at a few big properties in Las Vegas and New York. ALPHV/ BlackCat took responsibility for the attack. The attackers found the LinkedIn profile of an employee and then called the company help desk, in a practice known as social engineering. The company promptly informed the law enforcement agencies and took the help of cybersecurity experts.[17,18,19]
- On Sept 1, Zaun, a British mesh fencing systems maker disclosed it was the target of the LockBit ransomware gang in August but was able to thwart it before any data was encrypted, and its services were not interrupted. It later admitted to some data being exfiltrated. The company specializes in high-security perimeter fencing products used by prisons, military bases, and utilities.[20]
- On Aug 29, U.S.-based meal delivery service PurFoods revealed data pertaining to 1.2 million individuals was stolen in Feb 2023 in a ransomware attack. The stolen data included personally identifiable information (PII) and protected health information (PHI), including names, birth dates, social security numbers, driver's license numbers, payment card data, financial account information, and medical and health information. The organization has not disclosed if any ransom payment was made.[21]
- On Aug 18, Australian lender Latitude Financial in its financial report for H1 2023 revealed that a cyberattack resulted in AU$76 million ($50 million) in pre-tax costs and provisions to the company. The cyberattack exposed sensitive personal information belonging to 7.9 million people in Australia and New Zealand. The company received a ransom demand but refused to pay the attackers.[22]
- On Aug 18, Danish cloud hosting services provider CloudNordic announced that it lost all customer data following a ransomware attack that paralyzed the company's entire systems and servers. The attackers took advantage of an ongoing transition to a new data center and likely leveraged an existing, dormant infection to encrypt all systems. The company also mentioned that it has no plans to pay any ransom amount, although its investigation showed that it cannot recover the lost data.[23]
- On Aug 10, Japanese watchmaker SEIKO (TYO: 8050) revealed a data breach on July 28 that may have compromised information stored on its systems. BlackCat/ ALPHV started leaking files after the ransom payment was refused by the company. The 2 terabytes (TB) of stolen data included employee information, production technology details, video and audio recordings of management meetings, emails, and copies of passports belonging to employees and foreign visitors.[24]
- On Aug 7, U.S.-based Varian Medical Systems, a healthcare company specializing in providing software for oncology departments fell victim to the LockBit ransomware gang which threatened to leak the data of cancer patients, if the ransom amount was not paid.[25]
- On July 18, cosmetic giant Estée Lauder (NYSE: EL) disclosed a cyberattack by two cybercrime gangs. The CIOp gang claimed to have stolen 130 gigabytes of information through the MOVEit hack, which has impacted more than 400 organizations worldwide, while the BlackCat/ Alphv gang claimed to have

accessed the company's systems and threatened to leak the information if their demands were not met.[26]

- On July 5, the port of Nagoya in Japan was a victim of a ransomware attack. Japan's largest port in terms of cargo capacity had to suspend its cargo operations following the attack, which impacted its terminal system. The LockBit 3.0 ransomware gang may be responsible and made a ransom demand from the port authorities.[27]
- On June 29, Kinmax Technology admitted that its system was breached and some data relating to system installation preparation that it had provided to its customers was leaked. The LockBit ransomware group claimed responsibility and demanded $70 million in ransom payment. The company is one of the information technology (IT) hardware suppliers to Taiwan Semiconductor Manufacturing Company, (TSMC), (NYSE: TSM). TSMC in a statement mentioned that the breach did not affect its operations or compromise TSMC's customer information.[28]
- On June 28, energy giants Schneider Electric (EPA: SU) and Siemens Energy (ETR: ENR) confirmed being targeted by a CIOp ransomware group through exploiting a vulnerability in Progress Software's MOVEit, a type of managed file transfer (MFT) software. The energy giants are not alone and are among the 100 large organizations that fell victim to the MOVEit attack that was orchestrated last quarter. Siemens in a statement mentioned the attack did not have a significant impact on their operations and no critical data was infiltrated. With the number of confirmed organizations affected by the MOVEit attack reaching 400, the CIOp cybergang may have made up to $100 million in ransom money.[29,30]
- Quite a few medical centers and hospitals in the U.S. were targeted by ransomware groups. Some affected ones include Mount Desert Island Hospital in Maine, Kansas Medical Center in Kansas, HCA Healthcare in Tennessee, Panorama Eyecare in Colorado, Highland Health Systems in Alabama, Tampa General Hospital in Florida, McAlester Regional Health Center in Oklahoma, Prospect Medical Holdings in California, Oregon Sports Medicine in Oregon, and United Medical Centers in Texas. Others affected in other countries include Atherfield Medical and Skin Cancer Clinic in Australia and Luigi Vanvitelli Hospital in Italy.[31]

New Products

- Qualys Inc. (NASDAQ: QLYS) introduced its first-party software risk management solution in August 2023. This solution helps organizations to bring their own detection and remediation scripts, created using popular languages like PowerShell and Python, to Qualys Vulnerability Management, Detection, and Response (VMDR) as Qualys IDs (QIDs), which the Qualys Cloud Agent executes in a secure and controlled manner. The product further enables the customer to proactively detect, manage, and reduce supply chain risks as well as effectively communicate risk with Unified Reporting and Dashboarding.[32]
- Darktrace Plc. (NASDAQ: DARK) introduced its AI-based product HEAL™ in July 2023, which helps businesses to rapidly remediate and recover from cyber-attacks. According to the company, the product enables security teams to do the following:
    - I. Simulate real-world cyber incidents, allowing teams to prepare for and practice their response to complex attacks on their own environments;
    - II. Create bespoke, AI-generated playbooks as an attack unfolds based on the details of their environment, the attack, and lessons learned from their previous simulations. This reduces information overload, prioritizes actions, and enables faster decision-making at critical moments;

- III. Automate actions from the response plan to rapidly stop and recover from the attack within the HEAL interface; and
- IV. Create a full incident report, including an audit trail of the incident response with details of the attack, actions HEAL suggested, and actions taken by the security team for future learning and to support compliance efforts.[33]

- Splunk Inc. (NASDAQ: SPLK) has rolled out multiple cyber security products during its annual user conference 2023 (.conf23) in July 2023, which includes:
  - Splunk Edge Hub: a new solution that simplifies the ingestion and analysis of data generated by sensors, IoT devices and industrial equipment. It provides more complete visibility across IT and OT environments by streaming previously hard-to-access data directly into the Splunk platform.[34]
  - Splunk AI: a collection of new AI-powered offerings to enhance its unified security and observability platform. Splunk AI combines automation with human-in-the-loop experiences, so organizations can drive faster detection, investigation and response while controlling how AI is applied to their data.[35]
  - Splunk has introduced product innovations to its unified security and observability platform. According to the company, "the advancements span Splunk's portfolio and empower SecOps, ITOps and engineering teams with unified experiences and workflows so they can detect threats, investigate, and respond quickly, accurately, and at scale. These innovations build on Splunk's unified security and observability platform, and paired with Splunk AI offerings, provide organizations with unparalleled visibility across their hybrid environments to optimize costs, accelerate detection, investigation and response, and drive digital transformation".[36]
- Akamai Technologies (NASDAQ: AKAM) introduced its application programming interface (API) security product in August 2023, to protect APIs from business abuse and data theft. It stops API attacks and detects business logic abuse inside APIs. Additionally, it discovers, audits and monitors API activity using behavioral analytics to rapidly respond to threats and abuse.[37]
- CrowdStrike Holdings (NASDAQ: CRWD) introduced CrowdStrike Counter Adversary Operations in August 2023. This brings together CrowdStrike Falcon® Intelligence, the CrowdStrike Falcon Over Watch managed threat hunting teams, and AI. According to the company, "Counter Adversary Operations introduced its first new offering: Identity Threat Hunting, available as part of Crowdstrike Falcon OverWatch Elite. The offering brings together the latest intelligence on adversary TTPs and motives, combined with CrowdStrike Falcon Identity Threat Protection and CrowdStrike's elite Falcon OverWatch threat hunters to thwart the latest identity-based threats".[38]

Cybersecurity – M&A and IPO Activity in Q3 2023

Inside NQCYBR™ Index Activity:

- On Sept 21, Cisco (NASDAQ: CSCO) announced it had entered into an agreement to acquire Splunk (NASDAQ: SPLK) in a $28 billion all-cash deal. Splunk's artificial intelligence (AI), security and observability capabilities complement Cisco's offering and will boost its cybersecurity capabilities. The deal terms included paying $157 per share, a 31% premium to Splunk's prior day closing price. It is expected to close in Q3 2024.[39]

- On Sept 7, Tenable Holdings (NASDAQ: TENB) announced its intention to acquire Israeli cloud security startup Ermetic for ~$240 million in cash and $25 million in restricted stock. Ermetic provides a cloud-native application protection platform (CNAPP) and a cloud infrastructure entitlement management (CIEM) solution, and counts several Fortune 50 companies as its clients. Ermetic solutions is expected to boost the capabilities of the Tenable One exposure management platform, which includes vulnerability management, web app security, cloud security, identity security, attack surface management, and OT security capabilities. Tenable will pay the acquisition amount from its existing cash balances and the deal is expected to close in Q4 2023.[40]

- On Aug 10, network security company Check Point Software (NASDAQ: CHKP) announced its intention to acquire Secure Access Service Edge (SASE) and Zero Trust Network access (ZTNA) solutions provider Perimeter 81 for ~$490 million in a "cash free, debt free" deal. Perimeter 81 offers a platform that helps businesses to secure remote access, network traffic, and endpoint devices with its cloud-delivered Zero Trust Network Access, Firewall as a Service, and Secure Web Gateway (SWG) offerings. The acquisition was completed in mid-Sept.[41,42]

- On July 25, French aerospace, defense, and security giant Thales (EPA: HO) announced its intention to acquire U.S.-based cybersecurity company Imperva from Thoma Bravo for an enterprise value of $3.6 billion ($3.7 billion gross value minus $0.1 billion tax benefits). The transaction is expected to close by the beginning of 2024. Imperva offers application security, data security, network security and application performance solutions. The company's products are designed to protect applications and APIs against DDoS attacks, bots, and supply chain attacks; protect sensitive data in cloud and on-premises environments; and defend networks against DDoS attacks and ensure business continuity. Thoma Bravo acquired Imperva in 2018 for $2.1 billion in cash.[43]

- On Aug 25, private equity firm Veritas Capital made an offer to buy BlackBerry Ltd (NASADQ: BB), months after the Canadian technology company began a strategic review. BlackBerry first said in May it would consider strategic options for its portfolio of businesses that could include the possible separation of one or more of its businesses. Founded in 1984, and once the market leader in business smartphones, the company now makes software for cars and cybersecurity.[44]

Outside NQCYBR Index Activity:

- On Sept 11, Anteco Systems, S.L. (a/k/a AnyTech365), a leader in AI-powered IT security, and Zalatoris Acquisition Corp. (NYSE: TCOA), incorporated as a special purpose acquisition company in Delaware, entered into a business combination agreement. AnyTech365 IntelliGuard offers an AI-powered comprehensive threat prevention and performance enhancement optimization software. AnyTech365's subscription-based solutions are part of a Software-as-a-Service (SaaS) model. The transaction values AnyTech at an enterprise value of $220 million and the deal is expected to be completed in Q1 2024, subject to regulatory approvals.[45]

- On Aug 23, Parsons Corporation (NYSE: PSN) announced it had acquired U.S.-based cyber and technology company Sealing Technologies, Inc. (SealingTech) in a transaction valued at up to $200 million. SealingTech expands Parsons' customer base across the Department of Defense and Intelligence Community, and further enhances capabilities in defensive cyber operations. It integrated mission-solutions powered by AI and machine learning (ML); edge computing and edge access modernization; critical infrastructure protection; and secure data management. SealingTech will receive $175 million of cash at closing, with an additional $25 million earn out payable in Q1 2025 on meeting revenue targets during 2024. After factoring in a $21 million transaction-related tax benefit, the base purchase price implies a 10x multiple on SealingTech's forecasted 2023E adjusted EBITDA. SealingTech is expected to contribute $110 million to Parsons' revenue in 2024.[46]

Venture Capital and Other Private Equity Activity:

- On Sept 19, Secure Access Service Edge (SASE) solutions provider Cato Networks announced it raised $238 million at a valuation of more than $3 billion. The funding came from LightSpeed Venture Partners, with participation from Adams Street Partners, Softbank Vision Fund 2, Sixty Degree Capital, and Singtel Innov8, and brings the total amount raised by the company to $773 million. The funds would help to increase its customer base, expand its partner ecosystem for managed SASE services, and grow its engineering and product teams. The company's SASE platform provides secure web gateway (SWG), cloud access security broker (CASB), data loss prevention (DLP), zero trust network access (ZTNA), firewall-as-a-service (FWaaS), and remote browser isolation (RBI) capabilities.[47]

- On Sept 18, Dragos announced raising $74 million in Series D extension funding from WestCap. In the initial Series D funding in October 2021, it raised $200 million at a unicorn valuation of $1.7 billion. The latest funding brings the Series D round to $274 million, and the total funds raised to $440 million. The company specializes in protecting industrial control systems (ICS) and other operational technology (OT) against cyber threats. The funds will be used to help in additional go-to-market initiatives, accelerate expansion in North America, Europe, the Middle East and the APAC regions, as well as expansion across various industries. Dragos's industrial control systems (ICS)/ operational technology (OT) security platform provides asset visibility and inventory, vulnerability management, threat detection, and incident response capabilities.[48]

- On Aug 23, U.S.-based digital identity protection firm SpyCloud announced that it raised $110 million from Riverwood Capital. The company had previously raised more than $58 million in four funding rounds, including $30 million in a Series C round in 2020. The firm maintains a database of compromised assets and relies on the analysis of dark web data to identify and remediate exposed authentication and identity information. Its platform discovers stolen employee credentials, cookies, and other authentication data that threat actors use to target organizations and their customers, or the supply chain. The funds will help accelerate product innovation, release authentication bypass prevention solutions, expand its database of exposed assets, and improve its analytic capabilities.[49]

- On July 11, private equity (PE) firm Spire Capital announced that it acquired Israel-based web intelligence startup Cobwebs for $200 million. The company specializes in developing cyber intelligence solutions for enforcement bodies, national security agencies, and financial services worldwide, with a particular focus on the U.S. and Western Europe.[50]

- On July 10, PE giant TPG announced plans to acquire Forcepoint's Global Governments and Critical Infrastructure (G2CI) business unit from Francisco Partners in a deal reportedly valued in the range of $2.5 billion. G2CI was created in 2018 to serve as Forcepoint's government cybersecurity unit. TPG has plans to target the defense, intelligence and critical national infrastructure markets across the globe through the G2CI unit. The transaction is expected to close in Q4 2023 subject to regulatory approvals. Francisco Partners would retain a minority stake in the government-focused unit.[51]

[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.reuters.com/business/global-companies-hike-security-spending-threats-rise-survey-2023-09-11/
[8] https://www.cybersecuritydive.com/news/cisa-director-cyber-incident-reporting-infrastructure/693136/?&web_view=true
[9] https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html
[10] https://edition.cnn.com/2023/09/12/politics/department-of-defense-cyber-strategy-china/index.html

[11] https://www.securityweek.com/pentagons-2023-cyber-strategy-focuses-on-helping-allies/?web_view=true
[12] https://www.bankinfosecurity.com/uk-sounds-warning-over-targeted-healthcare-attack-a-22743?&web_view=true
[13] https://www.bloomberg.com/news/articles/2023-09-20/china-accuses-us-of-hacking-huawei-servers-as-far-back-as-2009#xj4y7vzkg
[14] https://www.bleepingcomputer.com/news/security/caesars-entertainment-confirms-ransom-payment-customer-data-theft/
[15] https://www.wsj.com/business/hospitality/caesars-paid-ransom-after-suffering-cyberattack-7792c7f0
[16] https://cybernews.com/security/caesars-palace-mgm-ransomware-attack-confirmed/
[17] https://www.securityweek.com/mgm-resorts-confirms-cybersecurity-issue-shuts-down-systems/
[18] https://www.bleepingcomputer.com/news/security/mgm-resorts-shuts-down-it-systems-after-cyberattack/
[19] https://www.securityweek.com/ransomware-gang-takes-credit-for-highly-disruptive-mgm-resorts-attack/
[20] https://www.securityweek.com/ransomware-attack-on-fencing-systems-maker-zaun-impacts-uk-military-data/
[21] https://www.securityweek.com/personal-health-information-of-1-2-million-stolen-in-purfoods-ransomware-attack/
[22] https://www.securityweek.com/australian-lender-latitude-financial-reports-au76-million-cyberattack-costs/
[23] https://www.securityweek.com/hosting-provider-cloudnordic-loses-all-customer-data-in-ransomware-attack/
[24] https://www.securityweek.com/ransomware-group-starts-leaking-data-from-japanese-watchmaking-giant-seiko/
[25] https://securityaffairs.com/149307/cyber-crime/varian-medical-systems-lockbit-ransomware.html
[26] https://www.securityweek.com/cosmetics-giant-estee-lauder-targeted-by-two-ransomware-groups/
[27] https://www.securityweek.com/japans-nagoya-port-suspends-cargo-operations-following-ransomware-attack/
[28] https://www.securityweek.com/tsmc-says-supplier-hacked-after-ransomware-group-claims-attack-on-chip-giant/
[29] https://www.securityweek.com/siemens-energy-schneider-electric-targeted-by-ransomware-group-in-moveit-attack/
[30] https://www.securityweek.com/moveit-hack-could-earn-cybercriminals-100m-as-number-of-confirmed-victims-grows/
[31] https://www.blackfog.com/the-state-of-ransomware-in-2023/#July
[32] https://investor.qualys.com/node/16826/pdf
[33] https://ir.darktrace.com/press-releases/2023/7/26/9d2dbe63702cd7c1512db60a9f96986ee7f2c088bf7b57dc97bb08c856f3ed51
[34] https://www.splunk.com/en_us/newsroom/press-releases/2023/conf23-splunk-introduces-new-ot-offering-to-enable-visibility-across-physical-and-industrial-environments.html
[35] https://www.splunk.com/en_us/newsroom/press-releases/2023/conf23-splunk-introduces-new-ai-offerings-to-accelerate-detection-investigation-and-response-across-security-and-observability.html
[36] https://www.splunk.com/en_us/newsroom/press-releases/2023/conf23-splunks-new-portfolio-innovations-deliver-unified-experiences-for-greater-customer-digital-resilience.html
[37] https://www.akamai.com/newsroom/press-release/akamai-announces-api-security-product-to-protect-api-from-business-abuse-and-data-theft
[38] https://www.crowdstrike.com/press-releases/crowdstrike-unleashes-new-counter-adversary-operations/
[39] https://www.securityweek.com/cisco-boosts-cybersecurity-capabilities-with-28-billion-splunk-acquisition/
[40] https://www.securityweek.com/tenable-to-acquire-cloud-security-firm-ermetic-for-240-million/
[41] https://www.securityweek.com/check-point-to-acquire-sase-security-firm-perimeter-81-for-490-million/
[42] https://www.checkpoint.com/press-releases/check-point-software-completes-acquisition-of-perimeter-81/
[43]https://www.securityweek.com/thales-acquiring-imperva-from-thoma-bravo-for-3-6-billion/
[44] https://www.privateequitywire.co.uk/veritas-eyes-blackberry-deal/
[45]https://www.accesswire.com/782603/anytech365-a-worldwide-leader-in-ai-powered-it-security-to-go-public-through-merger-with-zalatoris-acquisition-corp
46https://www.parsons.com/2023/08/parsons-acquires-sealing-technologies-inc/
[48] https://www.securityweek.com/sase-firm-cato-networks-raises-238-million-at-3-billion-valuation/
[49] https://www.securityweek.com/ics-security-firm-dragos-raises-74-million-in-series-d-extension/
[50]https://www.securityweek.com/digital-identity-protection-firm-spycloud-raises-110-million/
[51]https://www.calcalistech.com/ctechnews/article/sj11008xsfh
[52] https://www.securityweek.com/tpg-to-acquire-forcepoints-government-cybersecurity-business-unit/