Q3 2022 Cyber Security Update

Cyber Security News

- Recent research (dated August 2022) from MarketsandMarkets (provides B2B research reports)[1] expects the cybersecurity market size to grow from current $173.5 billion to $266.2 billion in 2027, i.e. a compound annual growth rate (CAGR) of 8.9% during 2022-2027.[2] Moreover, the report indicates cloud-based security deployment to grow at the fastest pace during the period.[3] Based on security type, products catering to mobile applications are expected to attract the highest share of overall spending during 2022-2027, given their wide usage.[4] Furthermore, the highest level of growth is expected in the Asia Pacific region, as "the adoption of cyber security solutions has been motivated by the fact that the small and medium enterprises (SMEs) in the area are experiencing cyberattacks, including 74% of SMEs in India and New Zealand, 33% in Indonesia and South Korea, and 37% in Japan".[5]
- According to a recent article from Chuck Brooks (President of Brooks Consulting International), research shows that 93% of company networks, when hit by a cyberattack, can be breached at the network perimeter, allowing the attacker to gain access to local network resources.[6] A recent survey conducted by machine identity specialist Venafi with 1,000 global chief information officers (CIOs) finds that 82% of CIOs believe their organizations are vulnerable to cyberattacks.[7] Furthermore, only 50% of US companies have a cybersecurity plan and only 43% are financially prepared for a cyberattack in 2022; last year, among reported cyberattacks, the cost to US businesses was more than $6.9 billion. In 2022, a higher percentage of attacks were disclosed, driven by the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) and the Securities Exchange Commission's (SEC) planned cyber-disclosure rule.[8, 9]
- The Russian invasion into Ukraine has led to an increase in cyberattacks on countries supporting Ukraine. Russian hacker groups such as XakNet and Killnet are targeting countries supporting Ukraine.[10] Killnet's recent attacks include disrupting 130 websites (in public and private sectors) in Lithuania. Recent attacks on websites in Germany, Italy, Romania, Norway, and the US were all linked to Killnet.[11]
- US National Cyber Director Chris Inglis has travelled to Israel, the Netherlands, and the UK during June-July 2022 to meet with government officials, private sector executives, and academic thought leaders to strengthen partnerships to ensure better cybersecurity ecosystems and to support US interests abroad.[12] According to the National Conference of State Legislatures (NCSL), so far in 2022 at least 40 states and Puerto Rico have introduced or considered more than 250 bills or resolutions that deal significantly with cybersecurity; 24 states have enacted at least 41 bills.[13]
- In August 2022, the SEC charged 18 individuals and entities for their roles in a fraudulent scheme in which dozens of online retail brokerage accounts were hacked and improperly used to purchase microcap stocks to manipulate the price and trading volume of those stocks.[14] Also in August, the Cybersecurity & Infrastructure Security Agency (CISA) issued a toolkit for the US midterm elections to enhance the cybersecurity and cyber resilience of the election infrastructure.[15]
- The US House of Representatives passed two cybersecurity bills in July 2022. The first bill authored by Congressman Bilirakis will require the Federal Trade Commission to report cross border complaints involving ransomware and other cyberthreat incidents. The second bill – the Energy Cybersecurity University

Leadership Act – directs the Department of Energy to establish an energy cybersecurity university leadership program.[16]

- In Europe, the European Commission is advancing two major pieces of legislation regarding operational resilience and cybersecurity: DORA (Digital Operational Resilience Act) and the NIS2 (Network and Information Security). Both are expected to have their final drafts published by the end of 2022.[17]

Notable Attacks & Breaches

- On September 6, **Samsung** US disclosed a data breach in late July where some customers' personal data were compromised. However, social security and credit card details were not stolen as per company claims. This is the second security breach at Samsung in 2022, following the earlier one in March that resulted in the online leaking of Samsung source code by the Lapsus$ ransomware gang.[18]
- On September 4, **KeyBank** revealed a cyberattack on July 5 where social security numbers, addresses and account numbers of some of their mortgage customers were stolen by breaking into computers at the insurance services provider Overby-Seawell Company. The information may have been stolen in furtherance of commiting financial fraud.[19]
- In August, the government agencies of two countries were targeted by cyber gangs. **Chile's** Ministry of Interior reported that Sernac (country's National Consumer Service) was a target of the RedAlert ransomware gang, who is believed to have encrypted the files. Similarly, in **Dominican Republic** the Ministry of Agriculture's Dominican Agrarian Institute (IAD) was hit by Quantum ransomware, with $650,000 demanded as a ransom payment.[20]
- The **government of Montenegro** was the latest victim when it suffered a cyberattack in its critical infrastructure causing damage and disruptions. The attack is believed to have happened on August 19, and was reported to the press on August 31. The Cuba ransomware gang claimed responsibility for stealing financial documents, correspondence with banks, balance sheets, tax documents, compensation, and even source code and demanded a ransom payment of $10 million.[21]
- Italy's oil giant **Gestore dei Servizi Energetici SpA** (GSE) was attacked by the BlackCat/ALPHV ransomware gang on August 28, which claimed to have stolen 700 gigabytes (GB) of data. The stolen files contained confidential data, including contracts, reports, project information, accounting documents, and other internal documentation.[22]
- On August 26, Portuguese state-owned flag carrier airline **TAP Air Portugal** fell victim to cybercriminals. The company said that no data was infiltrated and operations remained normal. On August 31, the Ragnar Locker ransomware gang claimed on their leaks website that the airline's systems were, in fact, breached – and posted some of the exfiltrated customer data.[23]
- On August 25, French hospital **The Center Hospitalier Sud Francilien** (CHSF) was a victim of a cyberattack resulting in patients being referred to other medical centers and postponing appointments for surgeries. The ransomware gang demanded a payment of $10 million in exchange for the decryption key.[24]
- On August 20, Greece's largest natural gas distributor **DESFA** revealed a cyberattack breaching their information technology (IT) systems with a possibility of data leakage. The confirmation of the attack came after the Ragnar Locker ransomware group leaked 360 GB of data on August 19. The company takes a strong stance against negotiating with cybercriminals and payment of any ransom.[25, 26]

- On August 18, the Wall Street Journal reported that starting on March 31, 2023, **Lloyd's of London Ltd.** Will have a new policy to exclude catastrophic state-backed cyberattacks from insurance coverage going into effect. Lloyd's cited the vast economic damages resulting from war-related cyberattacks.[27]
- On August 18, **Estonia** reported that it had blocked a massive cyberattack attempt on its public institutions and the private sector from Russian cybercriminals, and was able to prevent any impact to operations. Russian hacker group Killnet claimed responsibility, and mentioned it was in retaliation for the Baltic state's removal of a Soviet-era World War II memorial that week.[28]
- On August 15, **South Staffordshire Water**, a major supplier of drinking water to residents in the UK, confirmed a cyberattack disrupting their IT systems. Company officials stated that the water supply remained operational. Apparently, the Clop gang wanted to target Thames (one of the largest drinking water suppliers in the UK) but misidentified Staffordshire as its victim.[29]
- On August 10, **Cisco Systems** (NASDAQ: CSCO) revealed a cyberattack from May 2022 where 2.8 GB was believed to have been stolen. Yanluowang ransomware group gained access to Cisco's internal systems using stolen credentials after hijacking an employee's personal Google account. The files published by the gang on August 10 contained non-sensitive data which the company confirmed as originating from their networks.[30, 31]
- On August 8, **7-Eleven** had to shut down 175 of its stores based in Denmark due to a cyberattack. Other than revealing that their systems were locked and they were unable to use cash registers or receive payments, the company did not know the attacker's identity or the extent of any stolen data.[32]
- On August 8, **Bombardier Recreational Products** (BRP) reported a breach of its systems via a supply chain attack that put a temporary halt of some production sites. On August 15, the company provided information on resuming production at sites in Canada, Finland, the U.S., and Austria, while others were due to resume later that week. The RansomEXX gang began leaking 29.9 GB of allegedly stolen data from the firm.[33]
- On August 4, **Twilio** (NYSE: TWLO) became the latest victim among 130 other organizations (including MailChimp and Klaviyo) in an **Okta** (identity and access management provider) phishing campaign that hackers have been repeatedly deploying. The Twilio case involved an SMS-based phishing campaign aimed at tricking its employees into sharing their credentials. The phishing kit codenamed '0ktapus' has been underway since March 2022, targeting Okta identity credentials and 2FA codes, and carrying out subsequent supply chain attacks. Based on the phishing domains created in this campaign, the threat actors targeted companies in multiple industries, including cryptocurrency, technology, finance, and recruiting.[34, 35]
- On August 4, **Advanced** – the software supplier to the UK's National Health Service (NHS) – suffered a cyberattack causing widespread outages across NHS. Services impacted included patient referrals, ambulance dispatch, out-of-hours appointment bookings, mental health services and emergency prescriptions. The nature of the attack and the identity of the attackers were yet to be ascertained as per news articles dated August 11.[36]
- On August 1, German power electronics manufacturer **Semikron** disclosed a cyberattack. According to Bleeping Computer, LV ransomware appears to have been involved and the attackers claimed to have stolen 2 terabytes (TB) of files from the company's systems.[37]
- Luxembourg's electricity networks and natural gas pipelines company **Creos**, with operations in 5 European countries, was hit by a ransomware attack. Parent company **Encevo,** in public statements made on July 25, disclosed a cyberattack between July 22-23 that rendered their portals non-operational, although the supply of electricity and gas remained functional. On July 29, BlackCat/ALPHV claimed responsibility and

threatened to publish 150 GB of stolen sensitive data from Creos, including contracts, agreements, passports, bills, and emails. No figure on the ransom amount was disclosed by Encevo or the attacker.[38, 39]

- On July 19, German building materials giant **Knauf Group** reported a cyberattack that took place on June 29, forcing the company to shut down its IT systems. Black Basta took responsibility and published 20% of the stolen data with samples of email communication, user credentials, employee contact information, production documents, and ID scans displayed on the attacker's website.[40]
- On July 13, Japan-based game publishing giant **Bandai Namco** (TYO: 7832) confirmed that they were the target of cyber gangs on July 3. The BlackCat ransomware gang later claimed to have stolen corporate and customer personal data during the attack, but had not released anything as of July 13.[41]
- On July 6, US-based **SHI International**, a provider of IT products and services with $12.3 billion in annual revenue and operations in the US, the UK, and the Netherlands, confirmed a cyberattack. The company was forced to take some of its systems offline, including public facing websites and email, though none of its data was infiltrated as per company claims.[42]

New Products

- In August 2022, **Qualys** introduced its CyberSecurity Asset Management 2.0, which will help "security and IT teams to continuously discover unknown internet-facing assets and automatically assess their risk posture".[43] Qualys has introduced the product by integrating External Attack Surface Management (EASM) capabilities into the Qualys Cloud Platform.[44]
- During July 2022, **Darktrace** launched its interconnected set of artificial intelligence (AI) products known as PREVENT with the aim of helping customers to pre-empt future cyber-attacks. Based on breakthroughs developed in the firm's Cambridge Cyber AI Research Centre and the capabilities gained through the acquisition of Cybersprint in March 2022, PREVENT uses AI to "think like an attacker," finding pathways to an organization's most critical assets from every angle. The product has already been used by organizations in the US (including the city of Las Vegas) and by Sedgwick, a leading provider of business solutions.[45]
- At the end of H1 2022, **Splunk** announced its new Splunk Security Cloud product, which according to the company, is "the only data-centric modern security operations platform that delivers enterprise-grade advanced security analytics, automated security operations, and threat intelligence with an open, unparalleled ecosystem." The introduction of the new product comes on the heels of its recent acquisition of TruStar, a cloud-native security company specializing in data-centric threat intelligence.[46]
- In September 2022, Wipro announced that it is collaborating with **Palo Alto Networks** in providing managed security and network transformation solutions like SASE (Secure Access Service Edge), as well as cloud security and next-generation security operations center (SOC) solutions for enterprises around the globe, which in turn will help enterprises accelerate their digital transformations.[47]
- In August 2022, power management company Eaton Corporation and **CyberArk** announced a collaboration to bring protection to utility transmission, distribution devices and networks. The collaboration includes CyberArk integration with Eaton's IED Manager Suite (IMS) for password and identity management.[48]

M&A and IPO Activity

Inside NQCYBR Index Activity:

- On August 3, Ping Identity (NYSE: PING), provider of the Intelligent Identity solution for the enterprise, announced that it entered into a definitive agreement to be acquired by Thoma Bravo, a leading software investment firm, for $28.50 per share in an all-cash transaction valued at an Enterprise Value of approximately $2.8 billion. The offer represents a premium of approximately 63% over Ping Identity's closing share price on August 2, 2022. The transaction, which was unanimously approved by the Ping Identity Board of Directors, is expected to close in the fourth quarter of 2022, subject to customary closing conditions, including approval by Ping Identity shareholders and regulatory approvals.[49]
- On July 12, **Thales** (EPA: HO), a global technology leader with more than €16 billion in revenue, entered into an agreement to acquire OneWelcome, a European leader in the fast-growing market of Customer IAM, for a total consideration of €100 million. OneWelcome's strong digital identity lifecycle management capabilities will support Thales's existing Identity services (secure credential enrollment, issuance and management, Know Your Customer, etc.) and offer the most comprehensive identity platform in the market. The deal is subject to regulatory approvals and is expected to be completed in the second half of 2022. Thales will be adding 1,000 employees in its cybersecurity division, among 11,000 people it plans to hire worldwide in 2022.[50, 51]

Outside NQCYBR Index Activity:

- On September 6, **Cerberus Cyber Sentinel Corporation** (NASDAQ: CISO), an industry leader in managed cybersecurity and compliance, completed the acquisition of NLT Secure, a cybersecurity company based in Chile that provides security solutions and managed services to companies in South America. Terms of the deal were not disclosed by either entity.[52]
- On July 5, **Infinigate**, the pan-European value-added distributor (VAD) of cybersecurity solutions, announced its intention to acquire Nuvias Group's cybersecurity and secure networking business. The merger of the two highly successful businesses, provided it clears all the regulatory approvals expected in Q4 2022, would create a cybersecurity powerhouse in Europe with estimated annual revenue of €1.4 billion. The acquisition would strengthen Infinigate's leadership position in Europe across cybersecurity, secure networking, and secure cloud. Both entities are leaders in the small and midsize business (SMB) segment.[53]

Venture Capital and Other Private Equity Activity:

- On September 7, **Cymulate**, a late-stage Israeli startup in the breach and attack simulation space, announced it raised $70 million, bringing the total amount the firm has raised since 2016 to $141 million. The Series D funding came from existing investor One Peak, as well as from Susquehanna Growth Equity (SGE), Vertex Ventures Israel, Vertex Growth and Dell Technologies Capital. The firms plan to utilize the funds for market expansion and global growth initiatives.[54]
- On August 18, **TXOne Networks** raised $70 million in a Series B funding round from TGVest Capital (a venture capital firm), adding to the $24 million it had previously raised. TXOne Networks, created in 2018 with dual headquarters in Texas and Taiwan, is a joint venture between cybersecurity firm Trend Micro and industrial networking solutions provider Moxa. The company offers security gateways, endpoint agents and network segmentation solutions designed to help organizations secure, control, and monitor equipment and

operational technology. The funding will help the company expand market share, hire new talent, and enhance its cybersecurity offering.[55]

- On August 4, Israel-based **Talon Cyber Security**, an enterprise secure browser startup firm, raised $100 million in a Series A funding round from Evolution Equity Partners, with participation from Ballistic Ventures, CrowdStrike's Falcon Fund, Merlin Ventures, SYN Ventures, and previous investors. The new funding takes the total raised to $126 million.
- On July 14, US-based **Bishop Fox**, an attack surface management pioneer, announced the raising of $75 million in Series B funding from Carrick Capital Partners. The total amount raised by the company stands at $100 million. The 17-year-old firm is known for its penetration testing and offensive security expertise. It launched the Cosmos attack surface management platform to automate the discovery and mitigation of security weaknesses. The funds raised will be utilized to hire new talent and expand the Cosmos platform's capabilities.[56]
- On July 8, US-based **Coalition**, one of the largest cyber insurance providers in the US and Canada, raised $250 million in a Series F funding round valuing the firm at $5 billion. The investment was funded by Allianz X, Valor Equity Partners, Kinetic Partners, and other existing investors. In its Series E round in September 2021, the company raised $205 million at a valuation of $3.5 billion. The total amount raised by Coalition as of July 8 was $755 million.[57]
- On July 6, US-based startup **Swimlane** raised $70 million in Series C funding from Activate Capital, with participation from existing investors Energy Impact Partners (EIP) and 3Lines Venture Capital. The total amount raised by the firm stood at $170 million. Swimlane's Turbine platform relies on low-code security automation to capture telemetry and combine it with human logic to generate actionable intelligence that can help accelerate incident response.[58]

[1] https://www.linkedin.com/company/marketsandmarkets
[2] https://www.marketsandmarkets.com/pdfdownloadNew.asp?id=505
[3] https://www.marketsandmarkets.com/pdfdownloadNew.asp?id=505
[4] https://www.marketsandmarkets.com/pdfdownloadNew.asp?id=505
[5] https://www.marketsandmarkets.com/pdfdownloadNew.asp?id=505
[6] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber- statistics-for-mid-year-2022-that-you-need-to-know/?sh=47a21a6c7864
[7] https://betanews.com/2022/05/31/82-percent-of-cios-believe-their-software-supply-chains-are-vulnerable/
[8] https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/cybersecurity/cybersecurity-legislation-preparing-for-increased-reporting-and-transparency
[9] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=47a21a6c7864
[10] https://www.wired.com/story/russia-hacking-xaknet-killnet/
[11] https://www.wired.com/story/russia-hacking-xaknet-killnet/
[12] https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/12/readout-of-national-cyber-director-chris-ingliss-travel-to-israel-and-europe/
[13] https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2022637922035.aspx
[14] https://www.sec.gov/news/press-release/2022-145
[15] https://www.cisa.gov/uscert/ncas/current-activity/2022/08/10/cisa-releases-cybersecurity-toolkit-protect-us-elections#:~:text=CISA%E2%80%94through%20the%20Joint%20Cyber,resilience%20of%20U.S.%20election%20infrastructure.
[16] https://www.securityweek.com/house-passes-cybersecurity-bills-focusing-energy-sector-information-sharing
[17] https://www.ey.com/en_no/financial-services/decoding-dora-and-nis2-how-can-your-organization-prepare
[18] https://www.securityweek.com/samsung-us-says-customer-data-compromised-july-data-breach
[19] https://www.securityweek.com/keybank-hackers-third-party-provider-stole-customer-data
[20] https://www.securityweek.com/ransomware-attacks-target-government-agencies-latin-america

[21] https://www.bleepingcomputer.com/news/security/montenegro-hit-by-ransomware-attack-hackers-demand-10-million/
[22] https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-italian-energy-agency/
[23] https://www.securityweek.com/ransomware-gang-claims-customer-data-stolen-tap-air-portugal-hack
[24] https://www.bleepingcomputer.com/news/security/french-hospital-hit-by-10m-ransomware-attack-sends-patients-elsewhere/
[25] https://www.bleepingcomputer.com/news/security/greek-natural-gas-operator-suffers-ransomware-related-data-breach/
[26] https://www.securityweek.com/ransomware-gang-leaks-data-allegedly-stolen-greek-gas-supplier
[27] https://www.wsj.com/articles/lloyds-to-exclude-catastrophic-nation-backed-cyberattacks-from-insurance-coverage-11660861586
[28] https://www.securityweek.com/estonia-blocks-cyberattacks-claimed-russian-hackers
[29] https://www.computerweekly.com/news/252523856/South-Staffs-Water-is-victim-of-botched-Clop-attack
[30] https://www.bleepingcomputer.com/news/security/cisco-hacked-by-yanluowang-ransomware-gang-28gb-allegedly-stolen/
[31] https://www.securityweek.com/ransomware-group-leaks-files-stolen-cisco
[32] https://www.bleepingcomputer.com/news/security/7-eleven-denmark-confirms-ransomware-attack-behind-store-closures/
[33] https://www.bleepingcomputer.com/news/security/ransomexx-claims-ransomware-attack-on-sea-doo-ski-doo-maker/
[34] https://thehackernews.com/2022/08/twilio-suffers-data-breach-after.html
[35] https://www.bleepingcomputer.com/news/security/twilio-hackers-hit-over-130-orgs-in-massive-okta-phishing-attack/
[36] https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it
[37] https://www.securityweek.com/power-electronics-manufacturer-semikron-targeted-ransomware-attack
[38] https://www.cybersecuritydive.com/news/encevo-creos-envovos-ransomware/628604/
[39] https://www.securityweek.com/luxembourg-energy-company-hit-ransomware
[40] https://www.bleepingcomputer.com/news/security/building-materials-giant-knauf-hit-by-black-basta-ransomware-gang/
[41] https://www.bleepingcomputer.com/news/security/bandai-namco-confirms-hack-after-alphv-ransomware-data-leak-threat/
[42] https://www.bleepingcomputer.com/news/security/it-services-giant-shi-hit-by-professional-malware-attack/
[43] https://www.qualys.com/company/newsroom/news-releases/usa/qualys-launches-external-attack-surface-management-easm/
[44] https://www.qualys.com/company/newsroom/news-releases/usa/qualys-launches-external-attack-surface-management-easm/
[45] https://darktrace.com/newsroom/prevent-loop-proactive
[46] https://www.splunk.com/en_us/blog/security/introducing-the-world-s-first-modern-cloud-based-secops-platform-splunk-security-cloud.html
[47] https://www.wipro.com/newsroom/press-releases/2022/wipro-and-palo-alto-networks-expand-alliance-to-deliver-managed-security-and-network-transformation/
[48] https://www.eaton.com/us/en-us/company/news-insights/news-releases/2022/eaton-collaborates-with-cyberark.html
[49] https://www.thomabravo.com/press-releases/ping-identity-to-be-acquired-by-thoma-bravo-for-2.8-billion

[50] https://cpl.thalesgroup.com/about-us/newsroom/thales-acquires-ciam-leader-onewelcome
[51] https://www.thalesgroup.com/en/global/group#:~:text=Thales%20is%20a%20global%20technology,future%20we%20can%20all%20trust
[52] https://www.globenewswire.com/news-release/2022/09/06/2510379/0/en/Cerberus-Sentinel-announces-acquisition-of-NLT-Secure.html
[53] https://www.realwire.com/releases/Infinigate-to-acquire-the-Nuvias-Group
[54] https://www.securityweek.com/cymulate-closes-70m-series-d-funding-round
[55] https://www.securityweek.com/txone-networks-scores-70m-series-b-investment
[56] https://www.securityweek.com/bishop-fox-lands-75-million-series-b-funding
[57] https://www.securityweek.com/cyber-insurance-firm-coalition-raises-250-million-5-billion-valuation
[58] https://www.securityweek.com/security-automation-firm-swimlane-closes-70-million-funding-round