Q4 2022 Cyber Security Update

Cyber Security News/Insight

- Revenues of the cybersecurity market are expected to grow to $159.8-$169.2 billion by the end of 2022, as per Statista and Gartner estimates.[1] The market grew at a compound annual growth rate (CAGR) of 10.8% during the period 2016 to 2021 to a market size of $139.0 billion in 2021. Going forward, the market is expected to grow at a CAGR of 10.9% during the period 2022-2027 (to $262.4 billion by 2027). The growth is expected to be led by cyber solution products with an estimated year-on-year (YoY) growth ranging from 14.7-15.2%, followed by security services segment growing at a range of 6.5-7.4%.[2] The United States is the largest market for cybersecurity with a projected market size of $63.2 billion in 2022, and is expected to grow at a CAGR of 10.1% during the period 2022-2027 to a projected market size of $102.3 billion by 2027.[3]
- According to Cybersecurity Ventures, cybercrimes are expected to cost about $7 trillion in 2022. Ransomware remains the most prevalent form of attack. Geopolitical events such as Russia's attack on Ukraine has spurred targeted cyberattack incidents particularly on infrastructure.[4] A McKinsey report predicts damage from cyber attacks to reach $10.5 trillion by 2025.[5] The estimated addressable market/opportunity for cybersecurity is a staggering $1.5-$2.0 trillion, with only ~10% of the market penetrated at current levels.[6]
- 2022 saw the passage of a number of cybersecurity legislations, with the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) being particularly noteworthy.[7] According to research published by the Wall Street Journal in November 2022, 54% of businesses now demonstrate readiness to report a cybersecurity incident within 72 hours.[8] Cybersecurity issues are also coming under the purview of The Department of Homeland Security. Congress passed a $858 billion annual defense policy bill in December 2022,[9] which includes several provisions for U.S. Cyber Command and other federal agencies such as the State Department, while codifying into law the State Department's cybersecurity bureau launched earlier this year. [10]
- According to The Washington Post, tens of thousands of websites belonging to governments and Fortune 500 companies are at a risk of a security breach from hosting of Twitter (TWTR) computer code, known as advertising pixel. The FBI has expressed deep concern about Apple (AAPL)'s end-end encryption feature for iCloud (expected to roll out by the end of this year), claiming that it will hinder its ability to protect the American people from cyberattacks and other crimes. [11]
- European Union (EU) is upgrading its bloc-wide cybersecurity framework in an effort to make its society more resilient to cyberattacks. In November 2022, the EU Parliament and European Council approved the implementation of a new policy known as the Network and Information Security Directive 2 (NIS 2.0) replacing the original 2016 NIS directive, which was introduced in 2016 as the first EU-wide cybersecurity legislation.[12]
- Singapore and Germany signed a mutual recognition arrangement in October 2022 for the use of cybersecurity labels issued by the Cyber Security Agency of Singapore (CSA) for consumer smart products. Smart devices will be rated according to their levels of cybersecurity provisions to help customers make an informed decision and incentivise manufacturers in making more secured products.[13]

Cybersecurity – Notable Ransomware Attacks and Breaches in Q4 2022

- On December 8, Acuity Brands (NYSE: AYI) with operations in North America, Europe and Asia, disclosed data security breaches in two separate incidents, one that occurred in October 2020 and another in December 2021. The compromised data included confidential information on current and past employees and members of Acuity's health plan. There was no indication of customer information being stolen. The attack may have been done by the Conti ransomware gang The company mentioned that it first informed its customers, partners and others about the breach in December 2021, and the new public disclosure is a follow-up to notify impacted associates and provide them with the necessary resources.[14]
- On December 6, the New Zealand government confirmed that a ransomware attack disrupted businesses and public authorities in the country. The cyberattack on the managed service provider (MSP) Mercury IT on November 30 affected several businesses, six health regulatory bodies and impeded access to patient data.[15]
- On December 5, a cyberattack at a hospital complex (consisting of Andre-Mignot Hospital, Richaud Hospital and the Despagne Retirement Home) in Versailles, near Paris resulted in cancelled operations and some patients being transferred- three from intensive care and three from the neonatal unit). For several months now, hospitals in France have been targeted by cybercriminals. The Corbeil-Essonnes hospital near Paris was attacked by a cybergang disrupting operations for several weeks. A ransom demand was made but since it was unpaid, confidential data on patients and staff was posted to the dark web.[16]
- On November 28, a cyberattack in September on the server of Southampton County in Virginia may have resulted in personal information being compromised including Social Security numbers. The county informed the affected individuals and also confirmed that some of the stolen data was posted online by the attacker LockBit 3.0 gang.[17]
- On November 8, Maple Leaf Foods (TSE: MFI), Canada's meat giant company revealed it fell victim to a cyberattack that resulted in system outages. The company upon learning of the breach immediately engaged the services of cybersecurity and recovery experts. The Black Basta group later claimed responsibility for the attack on the company.[18,19]
- On November 7, Canada's second largest supermarket and pharmacy chain Sobeys disclosed a cyberattack impacting some services at the stores and technical difficulties faced in fulfilling prescriptions. Computers were locked out in affected stores, with point-of-sale (POS) and payment processing systems still working as they were set-up to work on a separate network. The attack appears to be the work of the Black Basta ransomware gang, but no mention of the attack was mentioned on the gang's website.[20]
- On November 3, LockBit ransomware gang which had attacked the German based automotive giant Continental (ETR: CON) in August offered to sell the stolen data from its systems for $50 million if their demands were not met by the company. The company officials did not disclose any further details on the attack or the ransom payment demand.[21,22]
- A report published by cybersecurity firm Group-IB on November 3 revealed that a French-speaking cybergang may have stolen $30 million from banks and other organizations between 2019 and 2021. The cybersecurity company is aware of 30 successful attacks and in many cases the victims were targeted multiple times. The victims were mainly banks, financial services, mobile banking services, and telecom firms spread across 15 countries in Africa, Latin America, and Asia. The attackers are known to use old software flaws and widely available malware and tools.[23]

- On October 31, Multi-Color Corporation (MCC), a major label printing company informed its approximately 10,000 employees of a data breach exposing their personal information in a cyberattack that occurred on September 29.[24]
- On October 29, all trains operated by DSB, the largest train operating company in Denmark stopped due to a cyberattack on the third-party IT service provider Super. Train drivers used a mobile application provided by Supeo with access to critical operational information on speed limits and on work being done to the railroad. When the IT provider shut down its servers due to the attack, the application stopped working and drivers were forced to stop their trains.[25]
- On October 28, Germany based mining company Aurubis AG (ETR: NDA), the largest copper producer in Europe, discovered a cyberattack targeting its IT systems. The company immediately shut down its systems as a precaution, but it did not hamper the production process and incoming and outgoing of goods were maintained manually.[26]
- On October 21, Pendragon Group (LON: PLG), the second largest motor retailer in the UK, announced to The Times, UK, of a cyberattack from the LockBit ransomware gang that allegedly demanded $60 million as ransom. The company mentioned that the attack had no impact on the operations, with the hackers stealing 5% of their database.[27]
- On October 12, Medibank (ASX: MPL), one of the largest Australian private health insurance providers which counts the Australian Prime Minister as one of its customers, identified suspicious activity and shut down some of its systems. Medibank initially claimed that no data was compromised in the cyberattack but a week later the threat actor contacted and informed them of stealing 200 gigabytes of data that included personal, health related, and credit card information about their customers. On October 25, Medibank revealed that the cyberattack could cost $25-$35 million due to lack of cyberinsurance, regulatory/ litigation related costs and the need to offer financial support to affected customers. On November 7, Medibank revealed that data of 9.7 million customers was compromised in a cyberattack. On November 8, hackers began leaking sensitive data after Medibank refused to pay any ransom amount to BlogXX/REvil ransomware gang. On November 30, the gang dumped the last set of stolen data on the dark web after the $9.7 million ransom demand was denied.[28,29,30,31,32]
- On October 17, US-based healthcare provider Keystone Health informed its patients of a data breach it suffered between July 28 and August 22. The leaked information contained patient information, including names, Social Security numbers, and clinical information. Over 235,000 individuals were affected as notified by the provider to the US Department of Health and Human Services. The healthcare provider did not reveal if ransomware was involved.[33]
- On October 17, German-based wholesale chain Metro AG (ETR: B4B) operating 661 stores in 30 countries fell victim to a cyberattack disrupting store operations in Austria, Germany, and France. Offline payment systems were setup as a stop-gap measure and online orders were delayed due to the attack.[34]
- On October 14, Woolworths Group Ltd. (ASX: WOW) revealed a cyberattack and data breach at MyDeal impacting 2.2 million customers. The company had acquired an 80% stake in MyDeal in September 2022. The company also mentioned that Woolworths systems are separate from MyDeal, and the parent company remained unaffected by the attack. The breached data included general information, but no payments details were leaked as per company reporting.[35]
- On October 10, major US airport websites went offline after a cyberattack promoted by a pro-Russian cybergang known as "KillNet" published a list of sites encouraging its followers to attack them. The distributed denial of service (DDoS) attacks involve knocking a website by flooding it with traffic and taking

it offline. However, only public-facing websites of the airports which supply flight and services information were affected and it did not have any impact on operations.[36]

- On October 7, Toyota Motor Corporation (TYO: 7203) announced that customers' personal information may have been leaked after a T-Connect site's source code was found to have inadvertently been published on GitHub for a period of five years from 2017 to 2022. The source code contained the access key to the data server that stored customer details. "Toyota T-Connect is the automaker's official connectivity app that allows owners of Toyota cars to link their smartphone with the vehicle's infotainment system". The company also explained that customer names, credit card data, and phone numbers were not compromised as they weren't stored in the exposed database.[37]
- On October 7, hackers diverted more than $560 million worth of cryptocurrency from Binance Bridge after exploiting a vulnerability in the BSC (BNB Chain) Token Hub cross-chain bridge (blockchain bridge). Binance announced that it was able to recover some of the stolen amount.[38]
- On October 6, Lloyd's insurance group of London detected a cybersecurity incident and shut down its systems as a precaution. The company did not share any details, but a quick response and actions taken by the company indicated a possible ransomware attack.[39]

New Products

- Palo Alto Networks (NASDAQ: PANW) launched its medical Internet of Things (IoT) cyber security protection, a comprehensive zero trust security solution specifically for digital healthcare. The product's design takes into account the vulnerability of the healthcare sector to cyberattacks. .[40] The company released five machine learning powered next-generation firewalls (NGFWs) in November 2022 to provide protection against the most advanced and evasive threats. Palo Alto also introduced 5G-native security in November, which is touted to be the first in the industry and enables service providers and enterprises to secure their 5G networks.[41]
- Check Point Software (NASDAQ: CHKP) introduced its new cybersecurity solution Quantum Titan as a part of its cyber security platform in October 2022 which leverages artificial intelligence (AI) and deep learning to deliver threat prevention against advanced domain name system exploits (DNS) and phishing, as well as autonomous IoT security.[42,43]
- Akamai Technologies (NASDAQ: AKAM) has rolled out fully software-defined scrubbing centers in October 2022, strengthening its next generation distributed denial of service (DDoS) protection platform (Prolexic). The new product will help defend customers from the largest, multi-terabit attacks and provide better performance and reliability for online businesses of any size, anywhere on the planet.[44]
- In November 2022, Fortinet (NASDAQ: FTNT) launched its managed cloud-native firewall service, FortiGate Cloud-Native Firewall (FortiGate CNF) on Amazon Web Services (AWS). The product is intended to simplify network security operations. It uses AI for real-time detection and protection against internal and external threats.[45]

Cybersecurity – M&A and IPO Activity in Q4 2022

Inside NQCYBR Index M&A Activity:

- On November 18, Palo Alto (NASDAQ: PANW), the US-based cybersecurity giant, announced its plan to acquire early-stage Israeli startup Cider Security for $195 million in cash. The deal adds software supply

chain security capabilities to its Prisma Cloud platform. Cider Security was formed in 2020 and is backed by Tiger Global Management, Glilot Capital Partners and Glilot's early growth fund, Glilot+, and has raised $32 million in a Series A funding following $6 million in seed funding in March 2022. "The company's 'AppSec Operating System' offers a comprehensive view of the engineering ecosystem, to secure the entire application development process, from code to deployment".[46,47]

Outside NQCYBR Index M&A Activity:

- On October 12, private equity (PE) firm Thoma Bravo announced its intention to acquire identity and access management (IAM) solutions provider ForgeRock (NYSE: FORG). The deal is valued at $2.3 billion, with the PE firm prepared to pay $23.35 per share representing a premium of 53% over FORG's closing price on October 10. The deal is expected to close in H1 2023. FORG's identity security and management platform provides orchestration, access control and governance capabilities and claims to have more than 1,300 entities as its clients. FORG generated revenue of $177 million and had a loss of $48 million for the full year in 2021. This is the third identity-based cybersecurity acquisition announcement from Thoma Bravo in 2022, the earlier acquisitions being SailPoint for $6.9 billion (completed in August) and Ping Identity for $2.8 billion (completed in October).[48,49,50,51]

Venture Capital and Private Equity Activity:

- On December 13, US-based Synk, founded in 2015, announced that it had raised $196.5 million in a Series G funding valuing the firm at $7.4 billion., The total amount raised till date is over $1 billion. The current round of funding was led by QIA (Qatar Investment Authority), with participation from Boldstart Ventures, Evolution Equity Partners, G Squared, Irving Investors, Sands Capital, and Tiger Global. Synk's platform can be integrated in an organization's development tools, automation pipelines, and workflows to find and fix security defects in open-source software, containers, and infrastructure as code. Synk claims that their platform helps increase productivity and revenue of its 2,300 customers by securing the critical sections of their applications.[52]
- On December 7, US-based Drata, a security compliance and automation startup raised $200 million in Series C funding from existing investors ICONIQ Growth and GGV Capital with participation from Alkeon Capital, Cowboy Ventures, Salesforce Ventures, SentinelOne's S Ventures, FOG Ventures, and Silicon Valley CISO Investors (SVCI). The company counts Microsoft Chief Executive Officer Satya Nadella and Snowflake's Frank Slootman among its investors. The company plans to utilize the funds for research and development (R&D) and add tools and features for startups and auditors to automate mandatory compliance processes. Last November, in a Series B funding, the company raised $100 million at a $1 billion valuation. The new funding values the company upwards of $2 billion.[53]
- On November 16, Akeyless, an Israel-based start-up in the secrets management space, raised $65 million in venture capital that was led by NGP Capital. Early backers Team8 Capital and Jerusalem Venture Partners (JVP) also participated. The new funding takes the total amount raised by the firm to $80 million and will be utilized to develop technology to manage credentials, certificates, keys and other secrets flowing across multi-cloud and DevOps environments. Akeyless markets a secrets orchestration platform to unify multiple related use cases via a single product. According to Akeyless Chief Executive Oded Hareven, "Secret management should reduce the attack surface but existing solutions only increase it by creating additional infrastructure for teams to secure and maintain".[54]
- On November 15, US-based surface management pioneer Bishop Fox secured $46 million in funds adding to the $75 million Series B round funding raised earlier in 2022, and taking the total funds raised since its founding 18 years ago to $154 million. The funding was led by WestCap, with NextEquity Partners and Rockpool Capital' contributing to the latest round of funds. Bishop Fox is known for its

penetration testing and offensive security expertise, with its flagship platform performing more than 2.3 billion operations identifying 13,000+ exposures per week, helping security teams save more than 5,000 hours per year in vulnerability identification and triage.[55]

- On November 11, Laika announced that it had raised $50 million in Series C funding from Fin Capital with additional participation from new and existing investors, including Centana Growth Partners, Canapi, J.P. Morgan Growth Equity Partners, and ThirdPrime. Collectively, the total investment in the company stands at $98 million. The US-based firm was founded in 2019 and provides end-to-end software and services that ensure information security compliance through compliance automation and audit management, bringing all audits in a single place for easy progress tracking. The funds raised will be utilized for product development, sales growth, and marketing.[56]
- On November 4, US-based Apiiro announced it secured $100 million in Series B funding, taking the total amount the firm had raised since its founding in 2018 to $135 million. The latest round of funding was led by General Catalyst, with additional participation from Greylock and Kleiner Perkins. The firm provides cloud-native application security covering the entire development process, tackling security risks from design to code to cloud while improving software supply chain security. It plans to use the funds to enhance and develop next generation application security.[57]
- On October 27, Versa Networks announced it had raised $120 million in a pre-IPO funding round from BlackRock with participation from Silicon Valley Bank (SVB). The total amount raised by the company stands at $320 million. Versa Secure offers secure access service edge (SASE) solutions providing security, networking, and analytics through a single software operating system. The new investment will be used towards market strategies and enhance the company's offering.[58]
- On October 20, US-based data privacy firm Anonos announced it had raised $50 million in growth funding from GT Investment Partners and facilitated by Aon. The total funds raised by the company since its founding in 2012 stood at $70 million. The firm offers "a software platform that aims to protect data in use by applying pseudonymization and other techniques to transform the data into 'Variant Twins', representing non-identifiable but fully accurate assets".[59]
- On October 12, UK-based Immersive Labs announced that it had received a cash infusion of $66 million from Ten Eleven Ventures, with participation from existing investors Goldman Sachs Asset Management, Summit Partners, Insight Partners, Menlo Ventures, and Citi Ventures. The company has raised $189 million in total. The company's platform helps organizations to continuously assess and improve their workforce resilience.[60]
- On October 5, private equity firm Kohlberg Kravis Roberts & Co., (KKR) increased its stake in attack surface management firm NetSPI and invested $410 million. The new funding comes a year after KKR and Ten Eleven Ventures invested $90 million in the company. The US-based NetSPI's cloud-based delivery model allows a customer to continuously monitor their attack surface and execute attack strategies based on real-world scenarios. The security solutions offered by the company include Attack Surface Management, Penetration Testing as a Service (PTaaS), and Breach and Attack Simulation.[61]

[1] https://www.statista.com/outlook/tmo/cybersecurity/worldwide#revenue
[2] https://www.statista.com/outlook/tmo/cybersecurity/worldwide
[3] https://www.statista.com/outlook/tmo/cybersecurity/united-states
[4] https://www.secureworks.com/resources/rp-state-of-the-threat-2022
[5] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers
[6] https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers
[7] https://www.cisa.gov/circia
[8] https://www.wsj.com/articles/key-data-points-from-the-wsj-pro-cybersecurity-forum-11670434236
[9] https://www.reuters.com/world/us/us-house-backs-sweeping-defense-bill-voting-continues-2022-12-08/
https://www.washingtonpost.com/politics/2022/12/08/twitter-data-tracker-inhabits-tens-thousands-websites/

[12] https://www.weforum.org/agenda/2022/12/cybersecurity-european-union-nis/
[13] https://www.csa.gov.sg/News/Press-Releases/singapore-and-germany-sign-mutual-recognition-arrangement-on-cybersecurity-labels-for-consumer-smart-products
[14] https://www.securityweek.com/lighting-giant-acuity-brands-discloses-two-data-breaches
[15] https://www.securityweek.com/new-zealand-government-hit-ransomware-attack-it-provider
[16] https://www.securityweek.com/french-hospital-cancels-operations-after-cyberattack
[17] https://www.securityweek.com/virginia-county-confirms-personal-information-stolen-ransomware-attack
[18] https://www.securityweek.com/cyberattack-causes-disruptions-canadian-meat-giant-maple-leaf-foods
[19] https://www.securityweek.com/ransomware-gang-takes-credit-maple-leaf-foods-hack
[20] https://www.bleepingcomputer.com/news/security/canadian-food-retail-giant-sobeys-hit-by-black-basta-ransomware/
[21] https://www.bleepingcomputer.com/news/security/lockbit-ransomware-claims-attack-on-continental-automotive-giant/
[22] https://www.securityweek.com/ransomware-gang-offers-sell-files-stolen-continental-50-million
[23] https://www.securityweek.com/french-speaking-cybercrime-group-stole-millions-banks
[24] https://www.securityweek.com/label-giant-multi-color-corporation-discloses-data-breach
[25] https://www.securityweek.com/cyberattack-causes-trains-stop-denmark
[26] https://www.securityweek.com/copper-giant-aurubis-shuts-down-systems-due-cyberattack
[27] https://www.bleepingcomputer.com/news/security/pendragon-car-dealer-refuses-60-million-lockbit-ransomware-demand/
[28] https://www.securityweek.com/australian-health-insurer-medibank-targeted-cyberattack
[29] https://www.securityweek.com/data-breach-australian-health-insurer-impacts-4-million-customers-could-cost-35m
[30] https://www.securityweek.com/medibank-confirms-data-breach-impacts-97-million-customers
[31] https://www.securityweek.com/ransomware-gang-threatens-publish-medibank-customer-information
[32] https://www.securityweek.com/hackers-dump-australian-health-data-online-declare-case-closed
[33] https://www.securityweek.com/keystone-health-data-breach-impacts-235000-patients
[34] https://www.bleepingcomputer.com/news/security/wholesale-giant-metro-hit-by-it-outage-after-cyberattack/
[35] https://www.securityweek.com/retail-giant-woolworths-discloses-data-breach-impacting-22-million-mydeal-customers
[36] https://www.securityweek.com/us-airport-websites-hit-suspected-pro-russian-cyberattacks
[37] https://www.bleepingcomputer.com/news/security/toyota-discloses-data-leak-after-access-key-exposed-on-github/
[38] https://www.securityweek.com/binance-bridge-hit-560-million-hack
[39] https://www.securityweek.com/insurance-giant-lloyds-london-investigating-cybersecurity-incident
[40] https://www.paloaltonetworks.com/blog/2022/12/medical-iot-security-to-depend-on/
[41] https://www.paloaltonetworks.com/company/press/2020/palo-alto-networks-launches-industry-s-first-5g-native-security-offering--enabling-service-providers-and-enterprises-to-create-new-revenue-streams-while-securing-5g
[42] https://www.checkpoint.com/press-releases/check-point-software-brings-faster-ai-enabled-network-security-and-advanced-threat-prevention-for-on-premise-cloud-and-iot/
[43] https://www.checkpoint.com/press-releases/check-point-software-brings-faster-ai-enabled-network-security-and-advanced-threat-prevention-for-on-premise-cloud-and-iot/
[44] https://www.akamai.com/newsroom/press-release/akamai-announces-next-generation-ddos-defense-platform
[45] https://www.fortinet.com/corporate/about-us/newsroom/press-releases/2022/fortinet-launches-managed-cloud-native-firewall-service
[46] https://www.securityweek.com/palo-alto-acquire-israeli-software-supply-chain-startup
[47] https://www.securityweek.com/appsec-firm-cider-security-emerges-stealth-38-million-funding
[48] https://www.securityweek.com/thoma-bravo-take-iam-company-forgerock-private-23-billion-deal
[49] https://www.sailpoint.com/press-releases/thoma-bravo-completes-acquisition-of-sailpoint/
[50] https://press.pingidentity.com/2022-10-18-Thoma-Bravo-Completes-Acquisition-of-Ping-Identity
[51] Factset
[52] https://www.securityweek.com/snyk-raises-1965-million-74-billion-valuation
[53] https://www.securityweek.com/investors-pour-200m-compliance-automation-startup-drata
[54] https://www.securityweek.com/akeyless-raises-65-million-secrets-management-tech
[55] https://www.securityweek.com/bishop-fox-adds-46-million-series-b-funding-round
[56] https://www.securityweek.com/laika-raises-50-million-its-compliance-platform
[57] https://www.securityweek.com/cloud-native-application-security-firm-apiiro-raises-100-million
[58] https://www.securityweek.com/versa-networks-raises-120-million-pre-ipo-funding-round

[59] https://www.securityweek.com/anonos-raises-50-million-data-privacy-platform
[60] https://www.securityweek.com/immersive-labs-raises-66-million-cyber-workforce-resilience-platform
[61] https://www.securityweek.com/kkr-boosts-netspi-stake-410-million-investment