Q1 2022 Cyber Security Update

Cyber Security News

- Recent research (dated March 2022) from Thales (Euronext Paris: HO) reported that one in five (21%) global organizations* experienced a ransomware attack in the last year, with 43% of those experiencing a significant impact on operations. Additionally, nearly one in three global businesses experienced a data breach in the last 12 months. Relatedly, "51% of IT leaders agreed that it is more complex to manage privacy and data protection regulations in a cloud environment".[1]
- Given the increasing frequency of cyberattacks in the U.S and globally, President Biden and his administration continue to focus on cybersecurity as a top priority. In March 2022, the Securities and Exchange Commission (SEC) voted to propose two new cybersecurity rules for public companies:
    1. "Mandatory cybersecurity incident reporting: Material incidents would have to be reported on an 8-K form within four business days of the incident."
    2. "Required disclosures on company policies to manage cybersecurity risks: Companies must also provide updates on previously reported material cybersecurity incidents."[2,3]
- In order to raise visibility and awareness of cyber incidents in the U.S., Biden signed new cybersecurity legislation on March 15, 2022. The law mandates critical infrastructure operators to report hacks to the Department of Homeland Security within 72 hours, and within 24 hours in the case of a ransomware payment. The mandatory nature of the law is expected to provide better insights for any government agencies investigating and responding to cyber attacks.[4]
- Biden warned about the increased potential of Russian cyberattacks against U.S. businesses and critical infrastructure, following Western sanctions on Russia in the wake of the Ukraine invasion.[5] This was consistent with earlier warnings from CISA Director Jen Easterly and Energy Secretary Jennifer Granholm in the early days of the invasion. During the 2nd week of March 2022, Anne Neuberger – the deputy national security adviser for cyber and emerging technologies – stated that Federal agencies had already briefed more than 100 companies on the elevated threat of cyberattacks.[6]
- Also in March 2022, the U.K government added stringent telecom security rules to its existing Telecommunications (Security) Act, which was passed in November 2021 to help defend the country from cyberattacks. Digital Infrastructure Minister Julia Lopez said, "Our proposals will embed the highest security standards in our telecoms industry with heavy fines for any companies failing in their duties".[7]
- Also in March 2022, the European Commission (EC) proposed new cybersecurity rules to ensure uniform security measures across EU institutions, bodies, offices, and agencies. According to the EC, the proposed rules will "put in place a framework for governance, risk management and control in the cybersecurity area. It will lead to the creation of a new inter-institutional Cybersecurity Board, boost cybersecurity capabilities, and stimulate regular maturity assessments and better cyber-hygiene".[8]

** Per Thales: "Organizations represented a range of industries, with a primary emphasis on healthcare, financial services, retail, and technology, as well as federal government agencies."*

Notable Attacks & Breaches

- On March 22, Microsoft (NASDAQ: MSFT) became the latest victim of the Lapsus$ cybergang when they released 37 GB of source code stolen from the Azure DevOps servers for Bing, Bing Maps, and Cortana products. Lapsus$ managed to compromise the account of one of the company's employees. MSFT's cybersecurity response team were quick to control the damage and remediate the compromised account.[9]
- Japan-based Denso (Tokyo: 6902), one of the world's largest automotive components manufacturers, detected a breach of their systems on March 10 at their German unit by the Pandora ransomware gang. The company stated that the cyberattack did not cause any disruption to the facilities or the production plants at their German unit.[10]
- Bridgestone (Tokyo: 5108), one of the world's largest tire manufacturers, was revealed as the latest victim of a LockBit ransomware attack that took place on February 27 inside its Americas unit. The attack was made public on March 11. The nature of the stolen data and its impact on the company was unclear.[11]
- NVIDIA (NASDAQ: NVDA), one of the world's largest semiconductor companies, confirmed that some employee credentials were stolen in a cyberattack by Lapsus$ that occurred on February 23. Up to 1 terabyte of data may have been impacted, with Lapsus$ starting to leak the information online. NVIDIA does not expect any disruption to their business.[12]
- On February 28, Toyota Motors (Tokyo: 7203) reported that it was forced to halt their car production operations temporarily due to a system failure at one of its key plastic suppliers - Kojima Industries - due to a cyberattack. In total, operations were suspended on 28 production lines across 14 plants in Japan. The suspension of production is likely to result in a 5% drop in Toyota's monthly production in Japan and create challenges to Toyota's just in time (JIT) approach.[13]
- On February 25, insurance giant Aon (NYSE: AON) disclosed a cyberattack on its 8-K filing: "Although the Company is in the early stages of assessing the incident, based on the information currently known, the company does not expect the incident to have a material impact on its business, operations or financial condition."[14]
- Dragos, an industrial cybersecurity company, reported that threat groups have been targeting industrial control systems (ICS) or other operational technology (OT) environments. KOSTOVITE, ERYTHRITE and PETROVITE are the new groups discovered in 2021, with the first two managing to gain direct access into ICS/OT networks. PETROVITE has targeted mining and energy operations in Kazakhstan, while KOSTOVITE is known to target the renewable energy sector in North America and Australia. ERYTHRITE has reportedly targeted many organizations in the U.S. and Canada, including a Fortune 500 company, a large electrical utility, food and beverage companies, IT firms, oil and gas companies, and vehicle manufacturers. Including the above three, Dragos is currently tracking 18 such threat groups.[15]
- On February 4, Swissport International, an aviation services company operating in 50 countries, reported a ransomware attack on its IT infrastructure and services, causing flight delays. BlackCat ransomware group was responsible for the cyberattack and claimed to have accessed up to 1.6 terabytes of stolen data.[16,17]
- On February 22, Delta Electronics (Taiwan: 2308) – a large Taiwanese electronics company with $9 billion in annual revenues, supplying customers including Apple, Tesla, HP, and Dell – disclosed a cyberattack. The company did not name the attacker but CTWANT, a Taiwanese news outlet, attributed it to the Conti ransomware group. The company claims that only non-critical systems were impacted, and that it had hired the services of third-party security experts to help in the investigation and restoration of data.[18]

New Products

- In February 2022, Fortinet (NASDAQ: FTNT) announced its Next-Generation Firewall (NGFW, powered by Fortinet's purpose-built NP7 and CP9 security processing units), *FortiGate 3000F*. This product is intended to support organizations in building hybrid IT architectures.[19]
- In February 2022, CrowdStrike Holdings (NASDAQ: CRWD) announced the general availability of its endpoint detection and response (EDR) capabilities product, Falcon XDR. According to CRWD, the product will "improve threat visibility across the enterprise, simplify security operations and dramatically speed up response time, containment and remediation of the most sophisticated attacks".[20]
- In March 2022, Zscaler (NASDAQ: ZS) introduced three innovations (Private App Protection, Deception, and Privileged Remote Access Capabilities) to its Zero Trust Network Access (ZTNA) product, which is designed to replace legacy firewalls and VPNs.[21]

M&A and IPO Activity

Inside NQCYBR Index Activity:

- On March 15, SentinelOne (NYSE: S) announced plans to acquire Attivo Networks, a Silicon Valley startup that sells breach detection technology, for $616 million in a cash-and-stock deal. The acquisition would equip SentinelOne to become a full-service player in the lucrative XDR (extended detection and response) space. "With this acquisition, SentinelOne extends its AI-powered prevention, detection, and response capabilities to identity-based threats, setting the standard for XDR and accelerating enterprise zero trust adoption". Critical identity security is a fast-growing category with a protected total addressable market (TAM) of $4 billion. The acquisition is expected to close in the second quarter of 2022, subject to regulatory approvals.[22]
- On March 8, Google (NASDAQ: GOOGL) announced it will acquire Mandiant (NASDAQ: MNDT) in an all-cash deal for $5.4 billion, one of the industry's largest M&A transactions to date. Mandiant works with customers including InfoSys, OlyFed, and the Bank of Thailand. Mandiant will become part of Google Cloud, where it will offer advisory services to help companies reduce risk before, during, and after security incidents with additional threat detection, intelligence, and automated incident response tools. Google expects the deal to close later this year, subject to regulatory and shareholder approvals.[23,24]
- On February 23, Cloudflare (NYSE: NET) announced an acquisition of Area 1 Security for $162 million, of which 40-50% is payable in shares of Cloudflare's Class A common stock. The deal is expected to close in the second quarter of 2022. Area 1 Security has a cloud-native platform built to work alongside email programs to stop phishing attacks. Per Cloudflare: "Email is the largest cyber-attack vector on the Internet, which makes integrated email security critical to any true Zero Trust network. That's why today we're welcoming Area 1 Security to help make Cloudflare's platform the clear leader in Zero Trust".[25]
- On February 1, Check Point (Nasdaq: CHKP) acquired Israeli cybersecurity startup Spectral for $60 million. Spectral is developing a scanner that identifies errors in code development and security problems in other assets that lead to breaches. Spectral presents these problems on a custom-designed dashboard. Spectral's solution will be added to Check Point's CloudGuard cloud security platform.[26]

Outside NQCYBR Index Activity:

- On March 23, HUB Cyber Security, an Israeli company that develops confidential computing cybersecurity solutions, stated that it will be merging with Mount Rainier Acquisition Corp. (NASDAQ: RNER), a SPAC (special purpose acquisition company), in a deal valued at nearly $1.3 billion. The company specializes in protecting sensitive commercial information with an advanced encrypted computing solution designed to prevent hostile intrusions and thefts. The deal is expected to close in the third quarter of 2022.[27,28]
- On March 8, Axonius announced that it had raised $200 million in Series E funding that values the company at $2.6 billion, following previous raises of $195 million from investors. The Series E round was led by Accel, with participation from Bessemer Venture Partners, Lightspeed Venture Partners, Alkeon, Stripes, ICONIQ, DTCP, Silver Lake Waterman, Alta Park Capital, and Owl Rock. Axonius integrates with myriad data sources to give companies a full inventory of their assets, enabling them to mitigate any threats due to security gaps they uncover. Its customers include Schneider Electric, The New York Times, Wacom, and AB InBev.[29]
- On February 23, BlueVoyant announced that it had raised $250 million in Series D funding that values the company at more than $1 billion, following previous raises of $350 million. The round was led by private equity firm Liberty Strategic Capital and included backing from ISTARI, Eden Global Partners and 8VC. The funds will help the company expand product offerings across both internal security and external cyber risk management. BlueVoyant is known for providing internal security to customers through its managed detection and response (MDR) offering, but is now placing an equal emphasis on its external cyber risk management services.[30]
- On February 22, eSentire – a Canadian cybersecurity vendor backed by Warburg Pincus – reported that it bagged $325 million of financing from Georgian and Caisse de dépot et placement du Québec (CDPQ), valuing the company at upwards of $1 billion. The recent round of funding takes the total amount raised by eSentire to $411 million, while the company now boasts $100 million in annual recurring revenue primarily from the managed detection and response (MDR) category. The funds will be used for geographic expansion and building out its newer Atlas XDR SaaS offering.[31]
- On February 22, market security provider CHEQ raised $150 million in Series C funding from Tiger Global, bringing total funds raised to $183 million. The company's solutions use a mix of bot mitigation, user validation, and behavioral analysis to distinguish between good or bad traffic by running over 2,000 real-time cybersecurity challenges on website visitors to verify their legitimacy.[32]
- On January 4, Siemplify, a late-stage Israeli startup selling SOAR (security orchestration, automation, and response) technology, was acquired by Google (NASDAQ: GOOGL) in the company's latest push into the cybersecurity business. Financial terms of the deal were not disclosed, but reports in Israel have put the price tag for the acquisition in the area of $500 million. Google plans to pair Siemplify's SOAR technology with its own home-built Chronicle security analytics platform to "change the rules on how organizations hunt, detect, and respond to threats". The technology also helps improve security operations center (SOC) performance by reducing caseloads, raising analyst productivity, and creating better visibility across workflows.[33]

[1] https://www.businesswire.com/news/home/20220323005016/en/

[2] https://www.sec.gov/news/press-release/2022-20

[3] https://www.cnbc.com/2022/03/09/sec-votes-to-propose-new-cybersecurity-rules.html

[4] https://www.bloomberg.com/news/articles/2022-03-16/biden-signs-law-requiring-firms-to-report-hacks-in-72-hours

[5] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/

[6] https://www.whitehouse.gov/briefing-room/press-briefings/2022/03/21/press-briefing-by-press-secretary-jen-psaki-and-deputy-nsa-for-cyber-and-emerging-technologies-anne-neuberger-march-21-2022/

[7] https://www.gov.uk/government/news/tougher-telecoms-security-rules-to-defend-uk-from-cyber-attacks

[8] https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1866

[9] https://www.bleepingcomputer.com/news/microsoft/microsoft-confirms-they-were-hacked-by-lapsus-extortion-group/

[10] https://www.bleepingcomputer.com/news/security/automotive-giant-denso-hit-by-new-pandora-ransomware-gang/

[11] https://www.bleepingcomputer.com/news/security/bridgestone-americas-confirms-ransomware-attack-lockbit-leaks-data/

[12] https://www.securityweek.com/nvidia-confirms-employee-credentials-stolen-cyberattack

[13] https://www.bleepingcomputer.com/news/security/toyota-halts-production-after-reported-cyberattack-on-supplier/

[14] https://www.bleepingcomputer.com/news/security/insurance-giant-aon-hit-by-a-cyberattack-over-the-weekend/

[15] https://www.securityweek.com/increasing-number-threat-groups-targeting-ot-systems-north-america

[16] https://www.bleepingcomputer.com/news/security/swissport-ransomware-attack-delays-flights-disrupts-operations/

[17] https://www.bleepingcomputer.com/news/security/blackcat-alphv-claims-swissport-ransomware-attack-leaks-data/

[18] https://www.bleepingcomputer.com/news/security/taiwanese-apple-and-tesla-contractor-hit-by-conti-ransomware/

[19] https://investor.fortinet.com/news-releases/news-release-details/new-fortinet-firewall-increases-security-and-networking

[20] https://www.crowdstrike.com/press-releases/crowdstrike-announces-general-availability-of-falcon-xdr/

[21] https://ir.zscaler.com/news-releases/news-release-details/zscaler-unveils-industry-first-security-service-edge-innovations

[22] https://www.securityweek.com/sentinelone-acquire-attivo-networks-616m

[23] https://venturebeat.com/2022/03/08/google-to-acquire-cybersecurity-company-mandiant-for-5-4b/

[24] https://www.mandiant.com/company/press-release/mgc

[25] https://www.zdnet.com/article/cloudflare-acquires-area-1-security-for-162-million/

[26] https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-695277

[27] https://www.reuters.com/business/israels-hub-cyber-security-list-nasdaq-via-13-bln-spac-deal-2022-03-23/

[28] https://jewishbusinessnews.com/2022/03/24/israels-hub-security-hits-1-28-billion-valuation-with-spac-merger/?fr=operanews

[29] https://venturebeat.com/2022/03/08/axonius-which-brings-asset-visibility-to-complex-it-environments-raises-200m/

[30] https://venturebeat.com/2022/02/23/bluevoyant-lands-250m-to-manage-security-external-risk-for-customers/

[31] https://www.securityweek.com/mdr-vendor-esentire-banks-325m-unicorn-valuation

[32] https://venturebeat.com/2022/02/22/cheq-raises-150-million-to-detect-malicious-website-visitors/

[33] https://www.securityweek.com/google-acquires-siemplify-ambitious-cybersecurity-push