Cybersecurity: A Year in Review

Over the last year, cybersecurity has become an even more crucial part of everyday life and a top priority for businesses and governments around the world, following several critical attacks on both the public and private sectors. In a new twist, the use of cyber warfare as a Russian tactic in its invasion of Ukraine has prompted a further ramping up of cybersecurity-related efforts and spending in the near term, including increased government regulation and legislation, especially within Europe and the US. And the statistics speak for themselves. In March 2022, Thales Research 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. In terms of preparation, Venafi reports that only 50% of US companies have a cybersecurity plan and only 43% are financially prepared, as the total cost of cyberattacks in the last year has ballooned to more than $6.9 billion. The number of attacks (and, for organizations who are unprepared, the costs associated with them) is expected to grow exponentially as the methods and tactics used by sophisticated hackers continue to evolve, making cyber security a non-negotiable necessity in today's highly digitized world. The hacks and breaches witnessed over the last year have proven just how serious the implications can be for the functioning of the global economy, whether it's an attack on a natural gas supplier or a semiconductor manufacturer. We'll review some of the key developments across the cybersecurity theme over the last year, including some of the newest government regulations, notable hacks/breaches, and a flurry of M&A activity that signals ongoing maturation in an industry with strong fundamentals and a number of secular tailwinds for continued growth.

Ramped Up Regulation

Cybersecurity has become a top priority for President Biden over the last year in reaction to the increased number and overall sophistication of cyberattacks not only in the U.S. but globally. Research published by Check Point (CHKP) reports that cyber-attacks have increased by 16% worldwide since the start of the Russian war against Ukraine in February 2022. To raise visibility and awareness of cyber incidents in the U.S., Biden signed new cybersecurity legislation on March 15, 2022, mandating critical infrastructure operators to report hacks to the Department of Homeland Security within 72 hours, and 24 hours in the case of a ransomware payment. Also in March 2022, the Securities and Exchange Commission (SEC) voted to propose two new cybersecurity rules for public companies: Mandatory reporting of material cybersecurity incidents on an 8-K form within four business days of the incident; and Required disclosures on company policies to manage cybersecurity risks, including updates on previously reported material cybersecurity incidents. Additionally, the US House of Representatives passed two cybersecurity bills in July 2022. The first bill authored by Congressman Bilirakis requires 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. Ahead of the November US midterm elections, the Cybersecurity & Infrastructure Security Agency (CISA) has issued a toolkit to enhance the cybersecurity and cyber resilience of the election infrastructure.

Cyber efforts have increased outside of the U.S., as well. The U.K government added stringent telecom security rules to its existing Telecommunications (Security) Act in March of this year, which was originally passed in November 2021 to help defend the country from cyberattacks. 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 "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." In May 2022, the European Commission accepted a political agreement between the European Parliament and the EU Member States on a new directive of measures for existing rules on the security of network and information systems (NIS Directive) across the Union. This enhanced directive covers "medium and large entities from more sectors that are critical for the economy and society, including providers of public electronic communications services, digital services, wastewater, and waste management, manufacturing of critical products, postal and courier services, and public administration, both at a central and regional level." Government entities in smaller nations have found themselves increasingly exposed to cyber threats due to a lack of resources and spending on preventing breaches, ransomware, and other cyber-attacks. For example, 27 government entities in Costa Rica were under attack in April-May 2022, and some of the worst affected included the Ministry of Finance and its two portals, the Virtual Tax Administration Portal (public tax collection portal), and the Information Technology for Customs Control portal. The attack caused a delay in the payment of pensions, salaries, subsidies, and tax collection.

Notable Hacks & Breaches

Cyberattacks over the last year have touched virtually every industry in both the public and private sectors. Below are some of the more notable attacks across different industries around the world.

Finance: In October 2021, Coinbase, a leading cryptocurrency exchange, was breached, as unauthorized access took place across nearly 6,000 accounts and some accounts even had funds stolen.[1] The online trading platform, Robinhood, disclosed a data breach in November 2021 of nearly five million customers. Personal data, such as email addresses, names, and dates of birth, were accessed by an unauthorized party.[2]

Commodities: Natural gas supplier, Super Plus, was a victim of a ransomware attack in mid-December 2021 that caused a disruption to their systems. According to CPO Magazine, "Superior Plus is a multi-billion-dollar company supplying energy-related products and services to over 780,000 customer locations in the United States and Canada."[3] Danish wind turbine giant Vestas Wind Systems detected a cyber security breach on November 19, 2021, and immediately shut down its IT systems across multiple business units and locations.[4] The company later confirmed that ransomware was indeed used, and the incident resulted in data getting compromised, but the wind turbine and supply chain operations were unaffected.

Aviation: 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.

Semiconductors: 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, 2022. Up to 1 terabyte of data may have been impacted, with Lapsus$ starting to leak the information online.

Automobile Industry: 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 was expected to result in a 5% drop in Toyota's monthly production in Japan, creating challenges to Toyota's just in time (JIT) approach.

Technology: 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 was quick to control the damage and remediate the compromised account.

Colleges & Universities/Education: The BlackCat ransomware gang attacked Florida International University on April 11. The gang claims to have stolen 1.2 terabytes (TB) of contracts, accounting documents, social security numbers, email databases, and more from students, teachers, and staff. Cybersecurity experts confirmed that the stolen data included sensitive information from staff and students. Several other universities, colleges, and public school systems were targeted by cyber attackers in April and May. In the U.S., some of the victims included A&T University in North Carolina, Austin Peay State University in Tennessee, Kellogg Community College in Michigan, Mercyhurst University in Pennsylvania, Fort Summer Municipal schools in New Mexico, Washington Local Schools in Ohio, Martin University in Indianapolis, and North Orange County Community College in California. Other institutions affected outside the U.S. included De Montfort School in Eversham in the U.K. and Regina Public Schools in Canada

Government Agencies: On a day when the Costa Rica government elected its 49th president (May 8), it had to declare a national emergency after the country was attacked by the Conti ransomware gang. The gang published 97% of the 672 gigabytes (GB) of leaked data belonging to various government agencies. The Ministry of Finance was the first to get impacted and is still evaluating the magnitude of the cyberattack. The Conti gang demanded a $10 million ransom, which the government refused to pay.

Tourism: Italy's fifth most populous city of Palermo was under cyber-attack on June 3. Local IT experts were trying to restore the systems for several days, during which all services, public websites, and online portals remained offline (even beyond June 6 when it was first reported to the public). The city hosts 2.3 million tourists annually, all of whom could not access online bookings for tickets to museums and theaters, or even confirm their reservations at sports venues. Full-time residents were also impacted. On June 9, the Vice City ransomware group claimed responsibility for the attack and threatened to publish the leaked data if the ransom was not paid.

Health Care: On August 4, Advanced, the software supplier to 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 reported on August 11.[5]

Retail: On August 8, Denmark-based 7-Eleven had to shut down 175 of its stores due to a cyberattack. Other than revealing on August 10 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 and the data stolen.[6]

Utilities/Water: On August 15, South Staffordshire Water company supplying drinking water to residents in the UK confirmed of a cyberattack disrupting IT systems. But the company officials informed 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.[7]

M&A Activity

Despite a broad-based drop in global M&A activity over the past year, there has still been plenty of transaction volume within cybersecurity, especially from private equity sponsors and large-cap technology companies. We've outlined some of the most notable activity below in chronological order.

October 21, 2021: Akamai Technologies, Inc. (NASDAQ: AKAM) completed its acquisition of Guardicore, a Tel Aviv-based company, for $600 million. Guardicore's technology stops malicious lateral movement by creating silos between servers, operating systems, applications, and cloud instances. The acquisition bolstered Akamai's portfolio of "Zero Trust solutions to protect enterprises from damage caused by breaches like ransomware while safeguarding the critical assets at the core of the network."[8]

December 10, 2021: ManTech International Corporation (NASDAQ: MANT) completed the acquisition of Gryphon Technologies, an engineering firm specializing in "model-based systems engineering, predictive analytics, data/computational science, and cloud engineering solutions that drive mission success for an array of Department of Defense agencies."[9] Gryphon Technologies strengthened ManTech's capabilities in cybersecurity as they provide a "focus on cyber security for control systems of all Navy platforms and systems."[10]

January 4, 2022: 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 helps improve security operations center (SOC) performance by reducing caseloads, raising analyst productivity, and creating better visibility across workflows.

February 23, 2022: Cloudflare (NYSE: NET) announced the 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 closed in April. 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".

March 8, 2022: Google (NASDAQ: GOOGL) announced the acquisition of Mandiant (NASDAQ: MNDT) in an all-cash deal for $5.4 billion, one of the industry's largest M&A transactions to date; the deal was officially completed on September 13. Mandiant works with customers including InfoSys, OlyFed, and the Bank of Thailand. Mandiant is now part of Google Cloud, where it offers advisory services to help companies reduce risk before, during, and after security incidents with additional threat detection, intelligence, and automated incident response tools.

March 15, 2022: 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, which was completed in May 2022, equips 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.

April 6, 2022: Investment firm Turn/River Capital announced an acquisition of Israel-based Tufin (NYSE: TUFN), a security policy management firm, for $570 million in cash. The agreement included a 30-day "go-shop" period until May 5, 2022. The $13.00 per share all-cash offer represented a 44% premium over Tufin's closing share price on April 5, 2022, but still less than the $14.00 per share price when the company went public in April 2019. The deal came at a relatively low valuation multiple of 5x 2022 revenues (FY 2021 revenue at $110.9 million) when compared to other listed cybersecurity firms. The acquisition was completed in August 2022.

April 12, 2022: Investment firm Kohlberg Kravis Roberts & Co. (KKR) agreed to acquire privately-held Barracuda Networks from Thoma Bravo. Financial terms of the deal were not disclosed, but Reuters reported the value to be nearly $4 billion. Barracuda, founded in 2003, is best known for its email, web, and network security solutions, and counts more than 200,000 customers around the world. During Thoma Bravo's ownership, the company expanded and enhanced its cybersecurity offerings, generating annual revenues of approximately $500 million. KKR's investments in the cybersecurity sector also include Ping, Cylance, DarkTrace, ForgeRock, NetSPI and Optiv, among others.

May 16, 2022: ManTech International Corporation (Nasdaq: MANT) entered into a definitive agreement to be acquired by Carlyle (Nasdaq: CG) in an all-cash transaction valued at approximately $4.2 billion. "ManTech's talented employees and leadership team have built a remarkable Company with strong market positions across the federal government," said Dayne Baird, a Managing Director on Carlyle's Aerospace & Government Services team. "Through this partnership, we look forward to leveraging our sector expertise and resources to accelerate growth and innovation and to drive greater value for customers and employees." This deal closed on September 14, 2022.

May 26, 2022: Broadcom Inc. (Nasdaq: AVGO) announced its plans to acquire VMware, Inc. (NYSE: VWM), where Broadcom would acquire all outstanding shares of VMware in a cash and stock transaction valued at approximately $61 billion. Raghu Raghuram, Chief Executive Officer of VMware, said, "VMware has been reshaping the IT landscape for the past 24 years, helping our customers become digital businesses. We stand for innovation and unwavering support of our customers and their most important business operations and now we are extending our commitment to exceptional service and innovation by becoming the new software platform for Broadcom. Combining our assets and talented team with Broadcom's existing enterprise software portfolio, all housed under the VMware brand, creates a remarkable enterprise software player. Collectively, we will deliver even more choice, value and innovation to customers, enabling them to thrive in this increasingly complex multi-cloud era." The acquisition is subject to regulatory approvals and VMware shareholder approval and is expected to close in 2023.

June 7, 2022: IBM (NYSE: IBM) announced it will acquire Randori, an early-stage attack surface management (ASM) startup based in Boston, Massachusetts, signaling the IT giant's cybersecurity expansion initiatives. Randori sells technology to help defenders conduct simulated hacking attacks on a continuous basis, which IBM plans to fold into its own products. The employee skills Randori has will add to IBM's X-Force offensive cybersecurity team. The financial terms of the deal were not disclosed, but Randori raised approximately $30 million in venture capital funding since its launch four years ago, including a recent $20 million Series A round led by Harmony Partners.

July 12, 2022: 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 to add 1,000 to its cybersecurity division of the total 11,000 people it plans to hire worldwide in 2022.

[1] https://www.zdnet.com/article/coinbase-sends-out-breach-notification-letters-after-6000-accounts-had-funds-stolen/
[2] https://blog.robinhood.com/news/2021/11/8/data-security-incident
[3] https://www.cpomagazine.com/cyber-security/natural-gas-supplier-superior-plus-suffers-a-ransomware-attack-similar-to-colonial-pipelines/
[4] https://www.securityweek.com/wind-turbine-giant-vestas-confirms-ransomware-involved-cyberattack
[5] https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it
[6] https://www.bleepingcomputer.com/news/security/7-eleven-denmark-confirms-ransomware-attack-behind-store-closures/
[7] https://www.computerweekly.com/news/252523856/South-Staffs-Water-is-victim-of-botched-Clop-attack
[8] https://www.prnewswire.com/news-releases/akamai-technologies-completes-acquisition-of-guardicore-to-extend-its-zero-trust-solutions-to-help-stop-ransomware-301405500.html
[9] https://investor.mantech.com/press-releases/press-release-details/mantech-completes-acquisition-gryphon-technologies
[10] https://www.raymondjames.com/-/media/rj/dotcom/files/corporations-and-institutions/investment-banking/industry-insight/market-intel-report.pdf