University of Miami Law Review

Volume 78 | Number 3 Article 5

4-22-2024

Understanding Cyber Risk: Unpacking and Responding to Cyber Threats Facing the Public and Private Sectors

Lawrence J. Trautman
Prairie View A&M University

Scott Shackelford
Indiana University Kelley School of Business

Brian Elzweig
University of West Florida

Peter Ormerod
Northern Illinois University College of Law

Understanding Cyber Risk: Unpacking and Responding to Cyber Threats Facing the Public and Private Sectors

LAWRENCE J. TRAUTMAN,[*] SCOTT SHACKELFORD,[**] BRIAN ELZWEIG,[***] PETER ORMEROD[****]

[*] J.D., Oklahoma City University School of Law; MBA, The George Washington University; B.A., The American University. Professor Trautman is Associate Professor of Business Law and Ethics at Prairie View A&M University, Associate Professor – Texas A&M University School of Law (by courtesy), Affiliate Scholar – Ostrom Workshop Program in Political Theory and Policy Analysis – Indiana University, Bloomington, and is past president of the New York and metropolitan Washington/Baltimore chapters of the National Association of Corporate Directors (NACD). He may be contacted at Lawrence.J.Trautman@gmail.com.

[**] J.D., Stanford Law School; Ph.D., University of Cambridge; B.A. Indiana University. Professor Shackelford is Provost Professor of Business Law & Ethics, Indiana University Kelley School of Business; Executive Director, Ostrom Workshop; Executive Director, Center for Applied Cybersecurity Research. He may be contacted at sjshacke@indiana.edu.

[***] J.D., California Western School of Law; LL.M. (securities and financial regulation), Georgetown University Law Center; B.S., Florida State University. Professor Elzweig is Professor and a Research Fellow of the Askew Institute for Multidisciplinary Studies at the University of West Florida. He may be reached at belzweig@uwf.edu.

[****] J.D., The George Washington University Law School; B.A. (magna cum laude), The George Washington University. Professor Ormerod is Assistant Professor at Northern Illinois University College of Law. He may be contacted at ormerod.peter@gmail.com.

The authors wish to extend particular thanks to the following for their assistance in the research and preparation of this Article: First, for the opportunity to present an early draft of this paper before the 92nd Annual Conference of the Academy of Legal Studies in Business (ALSB) in Savannah, Georgia, and for all

Cyberattacks, data breaches, and ransomware continue to pose major threats to businesses, governments, and health and educational institutions worldwide. Ongoing successful instances of cybercrime involve sophisticated attacks from diverse sources such as organized crime syndicates, actors engaged in industrial espionage, nation-states, and even lone wolf actors having relatively few resources. Technological innovation continues to outpace the ability of U.S. law to keep pace, though other jurisdictions including the European Union have been more proactive. Nation-state and international criminal group ransomware attacks continue; Sony's systems were hacked by a ransomware group; MGM Resorts disclosed that recovery from their September 2023 hack may ultimately cost more than $100 million; serious server software Log4j exploit became evident; U.S. embassy phones are hacked; cyberwarfare is deployed by Russia in their invasion of Ukraine; and theft of valuable intellectual property due to cybersecurity breaches are reported.

This Article proceeds in seven parts. First, it provides an overview of the cyber threat environment. Second, it discusses the current cybersecurity legal landscape. Third, it introduces cybersecurity and corporate governance. Fourth, it discusses how corporate directors govern cybersecurity. Fifth, it explores the emerging cyber threat from nation-states and the impact of geopolitics on business. Sixth, it focuses on issues involved in identifying and responding to digital attacks. And last, it concludes. This Article adds to the important body of cybersecurity literature that explores the roles of government and business, particularly corporate directors, in the governance of data security.

---

those who kindly provided comments. Our thanks to Bob Blakely, Seletha Butler, Frederick R. Chang, Robert Chesney, Michele Hooper, Ron McCray, Mason J. Molesky, H. Justin Pace, Ruth Simmons, and Peter Swire. All errors and omissions are our own.

OVERVIEW

Cyberattacks, data breaches, and ransomware continue to pose major threats to businesses, governments, and health and educational institutions worldwide.[1] Ongoing successful instances of cybercrime involve sophisticated attacks from diverse sources such as

---

[1] *See* ROBERT AXELROD & RUMEN ILIEV, THE STRATEGIC TIMING OF CYBER EXPLOITS 9, 14 (2013); Laurie R. Blank, *Cyberwar versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace*, *in* CYBERWAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 76, 77 (Jens David Ohlin et al. eds., 2015); P.A.L. Ducheine et al., *Towards a Legal Framework for Military Cyber Operations*, *in* CYBER WARFARE: CRITICAL PERSPECTIVES 101, 103 (P.A.L. Ducheine et al. eds., 2012); Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 318–19 (2015); Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 837–39 (2012); Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1536, 1540–41 (2010); Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 439–46 (2012); AFRODITI PAPANASTASIOU, APPLICATION OF INTERNATIONAL LAW IN CYBER WARFARE OPERATIONS 9 (2010), http://ssrn.com/abstract=1673785; Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1504, 1506 (2013); Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269, 269 (2014); Scott J. Shackelford & Amanda N. Craig, *Beyond the New "Digital Divide": Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity*, 50 STAN. J. INT'L L. 119, 135 (2014); Christina Parajon Skinner, *An International Law Response to Economic Cyber Espionage*, 46 CONN. L. REV. 1165, 1167–70 (2014);

organized crime syndicates, actors engaged in industrial espionage, nation-states, and even lone wolf actors having relatively few resources.[2] Technological innovation continues to outpace the ability of U.S. law to adapt, though other jurisdictions, including the European Union, have been more proactive.[3] Nation-state[4] and international criminal group ransomware attacks continue.[5] Sony's systems were hacked by a Ransomware group;[6] MGM Resorts disclosed that

---

T.P., *Hello, Unit 61398*, ECONOMIST (Feb. 19, 2013), https://www.economist.com/analects/2013/02/19/hello-unit-61398; *Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology: Hearing Before the H. Subcomm. on Oversight and Investigations of the H. Comm. on Foreign Affs.*, 112th Cong. 112–14 (2011); Peter Sommer & Ian Brown, *Reducing Systemic Cybersecurity Risk* 9 (Org. for Econ. Coop. & Dev., Working Paper No. IFP/WKP/FGS(2011)3), https://www.oecd.org/sti/futures/globalprospects/46889922.pdf; Paul N. Stockton & Michele Golabek-Goldman, *Curbing the Market for Cyber Weapons*, 32 YALE L. & POL'Y REV. 239, 240–41 (2013); Peter P. Swire, *A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?*, 3 J. TELECOMM. & HIGH TECH. L. 163, 177–78 (2004); Titiriga Remus, *Cyber-Attacks and International Law of Armed Conflicts; a "Jus Ad Bellum" Perspective*, 8 J. INT'L COM. L. & TECH. 179, 180–81, 185–86 (2013); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 422–24 (2011).

[2] *See* sources cited *supra* note 1.

[3] *See infra* Section IV.K; *see also infra* Section VI.E.

[4] *See* Andrew E. Kramer, *Companies Linked to Russian Ransomware Hide in Plain Sight*, N.Y. TIMES (Dec. 6, 2021), https://www.nytimes.com/2021/12/06/world/europe/ransomware-russia-bitcoin.html; Dustin Volz, *China-Linked Trolls Try Fueling Divisions in U.S. Midterms, Researchers Say*, WALL ST. J. (Oct. 26, 2022), https://www.wsj.com/articles/china-linked-internet-trolls-try-fueling-divisions-in-u-s-midterms-researchers-say-11666777403.

[5] *See INTERPOL Working Group Highlights Cyber Threats Across the Americas*, INTERPOL (Sept. 19, 2022), https://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-Working-Group-highlights-cyber-threats-across-the-Americas; David S. Wall, *The Transnational Cybercrime Extortion Landscape and the Pandemic: Changes in Ransomware Offender Tactics, Attack Scalability and the Organisation of Offending*, 5 EUR. L. ENF'T RSCH. BULL. 45, 47–48 (2022); Lawrence J. Trautman, W. Gregory Voss & Scott Shackelford, How We Learned to Stop Worrying and Love AI: Analyzing the Rapid Evolution of Generative Pre-Trained Transformer (GPT) and its Impacts on Law, Business, and Society, 34 ALB. L.J. SCI. & TECH. (forthcoming), http://ssrn.com/abstract=4516154.

[6] *See* Andrew Williams, *Sony Hack: What Happened and Who is Behind It?*, STANDARD (Sept. 28, 2023), https://www.standard.co.uk/news/tech/sony-hack-what-happened-ransomed-vc-b1110035.html.

recovery from their September 2023 hack may ultimately cost more than $100 million;[7] serious server software Log4j exploit became evident;[8] U.S. embassy phones were hacked;[9] cyberwarfare was deployed by Russia in their invasion of Ukraine;[10] and theft of valuable intellectual property due to cybersecurity breaches has been reported.[11]

This Article proceeds in seven parts. First, it provides an overview of the cyber threat environment. Second, it discusses the current cybersecurity legal landscape. Third, it introduces cybersecurity and corporate governance. Fourth, is a discussion about how corporate directors govern cybersecurity. Fifth, it explores the emerging cyber threat from nation-states and the impact of geopolitics on business. Sixth, it focuses on issues involved in identifying and responding to digital attacks. And last, it concludes. This paper adds to the important body of cybersecurity literature that explores the roles of government and business, particularly corporate directors, in the governance of data security.

---

[7] *See* Katherine Sayre, *MGM Resorts Refused to Pay Ransom in Cyberattack on Casinos*, WALL ST. J. (Oct. 5, 2023), https://www.wsj.com/tech/cybersecurity/mgm-resorts-refused-to-pay-ransom-in-cyberattack-on-casinos-3a53fa6d.

[8] *See* Robert McMillan, *Software Flaw Sparks Global Race to Patch Bug*, WALL ST. J. (Dec. 12, 2021, 4:22 PM), https://www.wsj.com/articles/tech-giants-microsoft-amazon-and-others-warn-of-widespread-software-flaw-11639260827; Robert McMillan & Dustin Volz, *Hackers Backed by China Seen Exploiting Security Flaw in Internet Software*, WALL ST. J. (Dec. 15, 2021, 6:21 PM), https://www.wsj.com/articles/hackers-backed-by-china-seen-exploiting-security-flaw-in-internet-software-11639574405.

[9] *See* Katie Benner et al., *Israeli Company's Spyware Is Used to Target U.S. Embassy Employees in Africa,* N.Y. TIMES (Dec. 3, 2021), https://www.nytimes.com/2021/12/03/us/politics/phone-hack-nso-group-israel-uganda.html.

[10] *See* Kristen E. Eichensehr, *Ukraine, Cyberattacks, and the Lessons for International Law*, 116 AM. J. INT'L L. UNBOUND 145, 145–46 (2022); JAMES A. LEWIS, CYBER WAR AND UKRAINE 1, 1 (June 2022), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220616_Lewis_Cyber_War.pdf.

[11] *See* William Boston, *Volvo Hit by Cyber Theft of Intellectual Property*, WALL ST. J. (Dec. 10, 2021), https://www.wsj.com/articles/volvo-hit-by-cyber-theft-of-intellectual-property-11639167971.

I. CYBER THREATS ESCALATE

The never-ending parade of high-impact data breaches continues. Ransomware group RansomedVC claimed to have breached all of Sony's systems in September 2023.[12] Supposedly, because of Sony's refusal to pay a ransom, RansomedVC placed the data for sale, asking $2.5 million.[13] If the data was not purchased, then RansomedVC threatened to publicly leak the data.[14] A rival hacker, MajorNelson, alleged that RansomedVC are "scammers" and claimed instead that they had been the ones that had infiltrated Sony.[15] In an offer of proof, MajorNelson publicly released over three gigabytes of data it claims it recovered from hacking Sony's systems.[16] Sony only has stated that they are "currently investigating the situation."[17] The alleged attack on Sony's data is one of many recent cybersecurity attacks.[18] For perspective, we describe several recent high-profile cases, along with a few having particular historical importance: Log4j; Colonial Pipeline; SolarWinds; Stuxnet; and WannaCry. Exhibit 1 illustrates the number of records lost each year (in billions) for the period 2014 to 2021.

---

12 Williams, *supra* note 6.

13 *Id.*

14 *Id.*

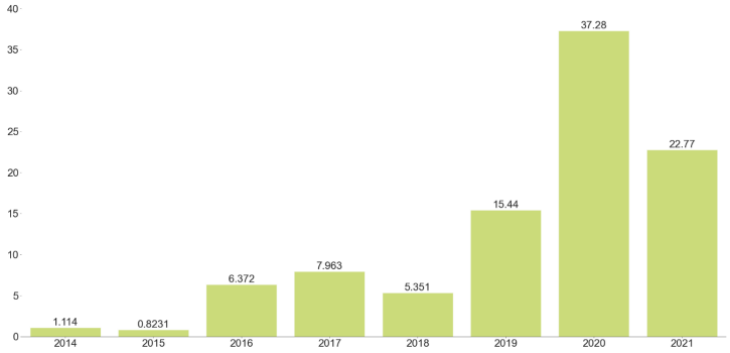
15 Ax Sharma, *Sony Investigates Cyberattack as Hackers Fight Over Who's Responsible*, BLEEPINGCOMPUTER (Sept. 26, 2023), https://www.bleepingcomputer.com/news/security/sony-investigates-cyberattack-as-hackers-fight-over-whos-responsible.

16 *Id.*

17 *Id.*

18 Wall, *supra* note 5, at 1.

EXHIBIT 1
The Number of Records Lost Each Year (in billions)
2014–2021[19]



For 2020, while the compromised records shown in Exhibit 1 "more than doubled from the previous year, the situation is not as atrocious as it appears, [as] 30.4 billion (or 82%) of the compromised records came from just five breaches."[20] "Misconfigured databases or services" accounted for all five of these breaches.[21] Details reveal that "the two largest breaches (accounting for 18.2 billion of the records exposed) also included a variety of logs."[22] RiskBased Security reported, "While this data is sensitive, especially so for the largest breach of the year which exposed user information from an adult entertainment site, there is scant evidence the data has been used for malicious purposes."[23]

Exhibit 2 depicts the number of vulnerabilities disclosed by Q4, for the period 2013 to 2020.

---

[19] RISKBASED SEC. & FLASHPOINT, 2021 YEAR END REPORT: DATA BREACH QUICKVIEW 10 (2022), https://go.flashpoint.io/l/272312/2022-06-23/24m8pjc/272312/1656014225Ciuuzgr4/2021_Year_End_Data_Breach_QuickView_Report.pdf.

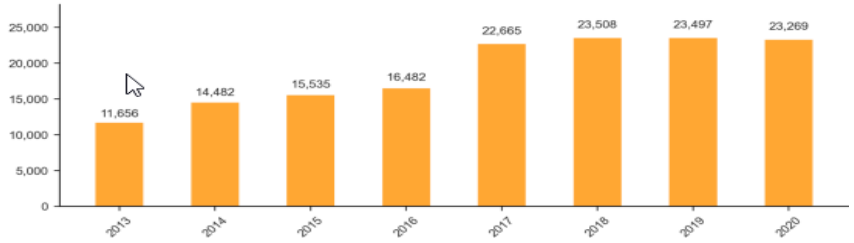
[20] RISKBASED SEC., 2020 YEAR END REPORT: DATA BREACH QUICKVIEW 12 (2021), https://go.flashpoint.io/l/272312/2022-06-23/24m8pj2/272312/1679927753gD6nDH7A/2020_Year_End_Data_Breach_QuickView_Report.pdf.

[21] *Id.*

[22] *Id.*

[23] *Id.*

EXHIBIT 2
The Number of Vulnerabilities Disclosed by Q4, 2013–2020[24]



The Covid-19 global pandemic appears to have impacted the results shown for Exhibit 2 in ways that might not be readily apparent. RiskBased Security reported that there "originally appeared to be a sharp decline in vulnerabilities in 2020 as compared to 2019: [I]n Q1 we saw a 19.2% drop, which is incredible. However, with each subsequent quarter that massive gap steadily closed, and . . . the 2020 vulnerability total is only 0.98% lower than 2019."[25] Following Covid-19, the Verizon 2023 Data Breach Investigations Report (DBIR) disclosed that "[f]inancial motives still drive the vast majority of breaches . . . with a whopping 94.6% representation in breaches . . . the top performer is organized crime."[26] Because of the Russian invasion of Ukraine, Verizon had expected increased state-sponsored activity; but, found, as shown by Exhibit 3, "it really isn't making a dent in larger statistical terms."[27]

---

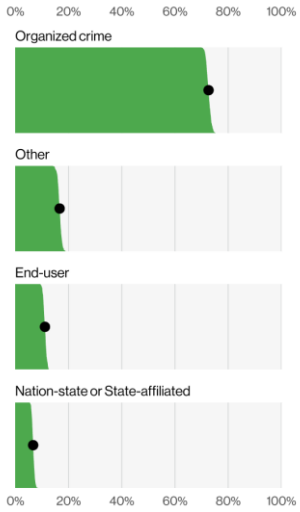
[24] RISKBASED SEC., 2020 YEAR END REPORT: VULNERABILITY QUICKVIEW 7 (2021), https://go.flashpoint.io/l/272312/2022-06-23/24m8phy/272312/1656014089l7GP4AqW/2020_Year_End_Vulnerability_QuickView_Report.pdf.

[25] *Id.*

[26] VERIZON, 2023 DATA BREACH INVESTIGATIONS REPORT 13 (2023), https://www.verizon.com/business/resources/T213/reports/2023-data-breach-investigations-report-dbir.pdf.

[27] *Id.*

EXHIBIT 3
Threat Actor Varieties in Breaches (n=2,489)[28]



For historical perspective, the evolution of nation-state-sponsored cyberattacks began in the waning days of the Bush Administration, when the malware known as "Operation Olympic Games" and more popularly as "Stuxnet" infected industrial control devices (programmable logic controllers) and was deployed against industrial machines used by Iran for the purification of radioactive uranium.[29] Trautman and Ormerod write, "By modulating the speed that Iranian centrifuges spun, Stuxnet covertly devastated the machines from within—representing the first time the world 'had seen digital code in the wild being used to physically destroy something in the real world.'"[30] The observations made during 2018 appear as relevant today:

---

[28] *Id.*

[29] Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, 72 U. MIA. L. REV. 761, 787–88 (2018) (citing DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER x (2012)); Derek E. Bambauer, *Schrödinger's Cybersecurity*, 48 U.C. DAVIS L. REV. 791, 794 (2015); William J. Broad et al., *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, N.Y. TIMES (Jan. 15, 2011), http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

[30] Trautman & Ormerod, *supra* note 29, at 788 (citing Kim Zetter, *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*,

> The Stuxnet virus represents a paradigm-shifting event. Stuxnet reveals to the world that a traditional military is no longer necessary to wreak havoc on other countries' military and civilian infrastructure installations. The implications for this shift are wide ranging and innumerable.
>
> Yet, the current climate within critical infrastructure industry fails to grapple with the ramifications of Stuxnet. Both industry and governments are unprepared to respond to a malware infection that renders worthless the systems that developed countries rely on for necessities as basic as food, water, telecommunications, and electricity.[31]

The ability to impact critical infrastructure can cause wide-ranging damage. Malware has been used in many cyberattacks aimed at destroying fundamental services.[32] Malware allows for attacks on infrastructure to be perpetrated by both state and non-state actors.[33] In 2013, an Iranian hacker, who was later found to be under orders of the Iranian military, hacked into the control systems of a Rye, New York, dam.[34] Although no damage was done, because the dam sluice gates were under maintenance, it showed that foreign actors were able to use cyberattacks to infiltrate portions of the United States' critical infrastructure.[35] The ability to breach these systems has led to attacks on a variety of essential functions such as "supplies and distribution of water and electricity, banking, communications, transportation and other systems vital to the everyday operation of

---

WIRED (July 11, 2011, 7:00 AM), https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet.

[31] *Id.* at 826.

[32] *See* Robert Kenneth Palmer, *Critical Infrastructure: Legislative Factors for Preventing a "Cyber– Pearl Harbor*,*"* 18 VA. J.L. & TECH. 289, 293 (2014)*; see also* Neal F. Newman, Lawrence J. Trautman & Brian Elzweig, The SEC Proposed Cybersecurity Infrastructure Rules and New Disclosure Requirements, (forthcoming), https://ssrn.com/abstract=4536669.

[33] *See* Carter D. Westphal, Comment, *Cyber Enablement and Control: Rehabilitating State Responsibility in Cyberspace*, 126 PENN ST. L. REV. 809, 818 (2022).

[34] *See id.* at 811.

[35] *See id.*

our government, economy and well-being."[36] Attacks on the infrastructure also have innumerable military uses.[37] In addition to direct hacking of a system, individuals and businesses must take steps to avoid illicit infringement on their data by exploitation through the Internet of Things ("IoT").[38] The IoT refers to "objects with sensors networked together that are capable of communicating with one another."[39] By breaching one of the interconnected devices, hackers can then use that breach to exploit weaknesses to gain access to other connected devices.[40] This access can become a gateway to all of an individual's connected devices, but could also become an entryway into a company's systems.[41] In the case of an individual, this would allow a hacker to exploit the multitude of data that people now have stored in devices.[42] However, if a hacker is able to breach a company's systems through the IoT, they would have access to proprietary company data and also vast amounts of customer data.[43] This data is valuable to people trying to exploit others, either by selling the data to third parties or by threatening to destroy the data and cause disruptions to the company.[44] This gives an avenue for malware to be implanted in an entity's systems, which can lead to other cybersecurity issues.[45] We will now look at examples of malware successfully deployed as ransomware.

---

[36] Palmer, *supra* note 32, at 293.

[37] *Id.* at 295.

[38] Jeremy Siegel, *When the Internet of Things Flounders: Looking into GDPR-Esque Security Standards for IoT Devices in the United States from the Consumers' Perspective*, 20 J. HIGH TECH. L. 189, 189 (2020).

[39] *Id.*

[40] Scott J. Shackelford & Scott O. Bradner, *Have You Updated Your Toaster? Transatlantic Approaches to Governing the Internet of Everything*, 72 HASTINGS L.J. 627, 634 (2021).

[41] Chynna Rose Foucek, *Cyber-Insecurity: The Reasonableness Standard in Internet of Things Device Regulation and Why Technical Standards Are Better Equipped to Combat Cybercrime*, 15 BROOK. J. CORP. FIN. & COM. L. 209, 211–15 (2020).

[42] *See id.*

[43] *See id.*

[44] *See* Margaret A. Reetz et al., *Cyber Risks: Evolving Threats, Emerging Coverages, and Ensuing Case Law*, 122 PENN ST. L. REV. 727, 731–33 (2018).

[45] *See id.* at 731–32.

A. *WannaCry and the Rise of Ransomware*

Companies that have been hacked are vulnerable to extortion through ransomware attacks.[46] Numerous recent attacks continue to target global and U.S. industry sectors, including "manufacturing, legal, insurance, health care, energy, education, and the food supply chain. . . . As Treasury Secretary Janet L. Yellen recently noted, 'Ransomware and cyberattacks are victimizing businesses large and small across America and are a direct threat to our economy.'"[47]

Trautman and Ormerod describe the ransomware attack known as WannaCry: "In August 2016, a group known only as 'the Shadow Brokers' began releasing and auctioning off a set of cyber weapons belonging to the U.S. National Security Agency's ('NSA') highly secretive Office of Tailored Access Operations ('TAO')."[48] The Shadow Brokers announced "a putative auction of digital weapons they claimed had been stolen from the 'Equations Group,' a highly advanced hacking group that many commentators believe is synonymous with the TAO."[49] During the second half of 2016, the Shadow Brokers "released a number of leaks . . . including digital tools for exploiting firewalls and network infrastructure engineered by companies that include Cisco, Juniper, Fortinet, and Huawei, a Chinese company."[50] During the years following WannaCry, "the

---

[46] *Id.* at 734.

[47] FIN. CRIMES ENF'T NETWORK, FINANCIAL TRENDS ANALYSIS: RANSOMWARE TRENDS IN BANK SECRECY ACT DATA BETWEEN JANUARY 2021 AND JUNE 2021 1 (2021) (citing Press Release, U.S. Dep't of Treasury, Treasury Takes Robust Actions to Counter Ransomware (Sept. 21, 2021), https://home.treasury.gov/news/press-releases/jy0364)); *see also* H. Justin Pace & Lawrence J. Trautman, *Financial Institution D&O Liability After* Caremark *and* McDonald's, 76 RUTGERS U. L. REV. 101, 142–43 (2023).

[48] Lawrence J. Trautman & Peter C. Ormerod, *WannaCry, Ransomware, and the Emerging Threat to Corporations*, 86 TENN. L. REV. 503, 523 (2019) (citing David E. Sanger, *'Shadow Brokers' Leak Raises Alarming Question: Was the N.S.A. Hacked?*, N.Y. TIMES, (Aug. 16, 2016), https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html).

[49] Trautman & Ormerod, *supra* note 48, at 523; Dan Goodin, *Confirmed: Hacking Tool Leak Came from "Omnipotent" NSA-tied Group*, ARS TECHNICA (Aug. 16, 2016), https://arstechnica.com/security/2016/08/code-dumped-online-came-from-omnipotent-nsa-tied-hacking-group.

[50] Trautman & Ormerod, *supra* note 48, at 523 (citing Lorenzo Franceschi-Bicchierai, *NSA Targeted Chinese Firewall Maker Huawei, Leaked Documents*

growing scale, scope, and severity of attacks by foreign hackers has brought to the fore the national-security implications of ransomware, compromising interstate infrastructure, food supplies, and health systems."[51] But even this breach is just one in a long list of troublesome, successful exploits.

B. *Log4j*

On December 13, 2021, the *Wall Street Journal* reported, "Companies and governments around the world rushed . . . to fend off cyberattacks looking to exploit a serious flaw in a widely used piece of Internet software that security experts warn could give hackers sweeping access to networks."[52] Of grave concern, this "Log4j" exploit "represents one of the biggest risks seen in recent years because the code is so widely used on corporate networks."[53] Just a few days later, it was reported that "[h]ackers linked to China and other governments are among a growing assortment of cyberattackers seeking to exploit a widespread and severe vulnerability in computer server software, according to cybersecurity firms and Microsoft Corp."[54] This followed an urgent statement on December 11, 2021, from Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency ("CISA"), which read:

> CISA is working closely with our public and private sector partners to proactively address a critical vulnerability affecting products containing the log4j software library. . . . We urge all organizations to join us in this essential effort and take action.[55]

Suggest, VICE (Aug. 24, 2016, 9:00 AM), https://www.vice.com/en/article/yp35pg/nsa-huawei-firewalls-shadow-brokers-leak).

[51] Ian Talley, *Suspected Ransomware Payments Nearly Doubled This Year, Treasury Says*, WALL ST. J. (Oct. 15, 2021, 3:28 PM), https://www.wsj.com/articles/suspected-ransomware-payments-for-first-half-of-2021-total-590-million-11634308503.

[52] *See* McMillan, *supra* note 8.

[53] *Id.*

[54] *See* McMillan & Volz, *supra* note 8.

[55] Press Release, U.S. Cybersecurity & Infrastructure Sec. Agency, Statement from CISA Director Easterly on Log4j Vulnerability (Dec. 11, 2021), https://www.cisa.gov/news-events/news/statement-cisa-director-easterly-log4j-vulnerability.

CISA recommends that asset owners take three additional, immediate steps regarding this vulnerability:

> 1. Enumerate any external facing devices that have log4j installed.
>
> 2. Make sure that your security operations center is actioning every single alert on the devices that fall into the category above.
>
> 3. Install a web application firewall (WAF) with rules that automatically update so that your SOC is able to concentrate on fewer alerts.[56]

This effort also underscores the urgency of building software securely from the start and more widespread use of Software Bill of Materials ("SBOM"), both of which were directed by President Biden in an Executive Order issued in May 2021.[57] A SBOM would provide end users with the transparency they require in order to know if their products rely on vulnerable software libraries.[58]

Brian Martin, Vice President of Vulnerability Intelligence at RiskBased Security, observed, "to qualify as a mega-vulnerability, entries need to have hundreds or even thousands of vulnerability references while affecting a tremendous amount of products and vendors. The accompanying charts illustrate how Log4Shell compares among its peer group."[59] On July 15, 2022, the *Wall Street Journal* reported, "A major cybersecurity bug detected last year in a widely used piece of software is an 'endemic vulnerability' that could persist for more than a decade as an avenue for hackers to infiltrate computer networks, a U.S. government review has concluded."[60]

---

[56] *Id.*

[57] *Id.*

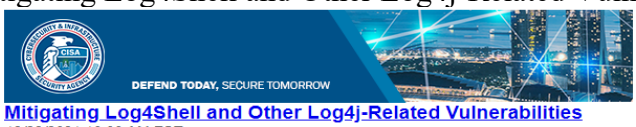
[58] BRIAN MARTIN, 2021 YEAR END VULNERABILITY QUICKVIEW REPORT: VULNERABILITY QUICKVIEW 4 (2022), https://www.flashpoint.io/resources/research/2021-year-end-report-vulnerability-quickview.

[59] *Id.*

[60] Dustin Volz, *Major Cyber Bug in Log4j to Persist as 'Endemic' Risk for Years to Come, U.S. Government Board Finds*, WALL ST. J. (July 14, 2022, 7:00 AM), https://www.wsj.com/articles/major-cyber-bug-in-log4j-to-persist-as-endemic-risk-for-years-to-come-u-s-government-board-finds-11657796400.

Exhibit 4 illustrates an example of a CISA advisory targeted toward Log4Shell and other Log4j-related vulnerabilities and procedures for detailed mitigations.

EXHIBIT 4
Mitigating Log4Shell and Other Log4j-Related Vulnerabilities[61]



Mitigating Log4Shell and Other Log4j-Related Vulnerabilities

12/22/2021 10:00 AM EST

Original release date: December 22, 2021
CISA, the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom have released a joint Cybersecurity Advisory in response to multiple vulnerabilities in Apache's Log4j software library. Malicious cyber actors are actively scanning networks to potentially exploit CVE-2021-44228 (known as "Log4Shell"), CVE-2021-45046, and CVE-2021-45105 in vulnerable systems. According to public reporting, Log4Shell and CVE-2021-45046 are being actively exploited.
This advisory expands on CISA's previously published guidance, drafted in collaboration with industry members of CISA's Joint Cyber Defense Collaborative (JCDC), by detailing recommended steps that vendors and organizations with information technology, operational technology/industrial control systems, and cloud assets should take to respond to these vulnerabilities.
CISA, FBI, NSA, the Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the Computer Emergency Response Team New Zealand (CERT NZ), the New Zealand National Cyber Security Centre (NZ NCSC), and the United Kingdom's National Cyber Security Centre (NCSC-UK) assess that exploitation of these vulnerabilities, especially Log4Shell, is likely to increase and continue over an extended period. CISA and its partners strongly urge all organizations to review AA21-356A: Mitigating Log4Shell and Other Log4j-Related Vulnerabilities for detailed mitigations.

RiskBased Security, Inc. reported:

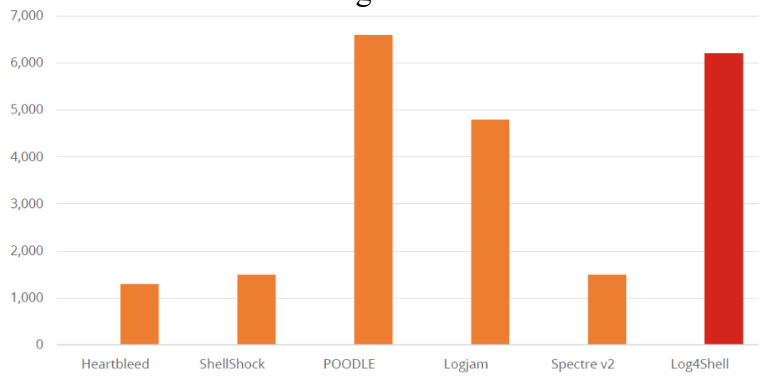
> Most mega-vulnerabilities take years to accumulate references and affected vendors/product information. But in just a month, Log4Shell has surpassed every other mega-vulnerability, except for one. [As of January 2022], there are over 1,850 vulnerability references specifically citing Log4Shell and its variants, and they affect over 6,200 vendors/product combinations. Of those, over 275 are unique vendors and 1,677 unique products, meaning that some organizations will likely be impacted several times over. In terms of affected vendors and products, Log4Shell falls slightly behind POODLE. However, if Log4Shell-related vendor advisories continue at their current pace, it will likely surpass POODLE within

---

[61] *Cybersecurity Advisory: Mitigating Log4Shell and Other Log4j-Related Vulnerabilities*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-356a (last updated Dec. 23, 2021).

> the next month. Nevertheless, the main highlight is the incredible amount of Log4Shell references circulating on the web. Out of all 280,000 known vulnerabilities, Log4Shell has the most references by a wide margin. This means that there is an incredible amount of existing information out there. But if that's the case, why are organizations seemingly struggling to mitigate and remediate affected assets?[62]

EXHIBIT 5
RiskBased Security Report of Total Number of Vulnerability References for Mega-Vulnerabilities[63]



C. *Colonial Pipeline*

On May 9, 2021, the *New York Times* reported, "One of the nation's largest pipelines, which carries refined gasoline and jet fuel from Texas up the East Coast to New York, was forced to shut down after being hit by ransomware in a vivid demonstration of the vulnerability of energy infrastructure to cyberattacks."[64] Within days, the FBI had attributed the attack to "a criminal gang of hackers called DarkSide . . . which first began to deploy such ransomware last August [2020], and is believed to operate from Eastern Europe,

---

62 MARTIN, *supra* note 58, at 5.

63 *Id.*

64 David E. Sanger et al., *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, N.Y. TIMES, https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html (last updated May 13, 2021).

possibly Russia."[65] Soon thereafter, Colonial Pipeline made a $4.4 million ransom payment.[66] Responsible for the supply of almost half the gasoline and diesel consumed on the East Coast of the United States, the Colonial Pipeline disruption had a ripple effect that impacted fuel prices and availability in the eastern United States for weeks.[67] At least two class action lawsuits[68] as well as several lawsuits by individual gas stations have been brought against Colonial Pipeline.[69] In a highly unusual development for most ransomware events, the U.S. Department of Justice announced it was able to recover much of the ransom paid by Colonial Pipeline.[70] Accordingly, the *New York Times* reported:

> Investigators in recent weeks traced 75 Bitcoins worth more than $4 million that Colonial Pipeline had paid to the hackers . . . Federal investigators tracked the ransom as it moved through a maze of at least 23 different electronic accounts belonging to DarkSide, the hacking group, before landing in one that a federal judge allowed them to break into, according to law enforcement officials and court papers.

---

[65] David E. Sanger & Nicole Perlroth, *F.B.I. Identifies Group Behind Pipeline Hack*, N.Y. TIMES (May 10, 2021), https://www.nytimes.com/2021/05/10/us/politics/pipeline-hack-darkside.html.

[66] Charlie Osborne, *Colonial Pipeline CEO: Paying DarkSide Ransom Was the 'Right Thing to Do for the Country*,*'* ZDNET (May 20, 2021, 4:04 AM), https://www.zdnet.com/article/colonial-pipeline-ceo-paying-darkside-ransom-was-the-right-thing-to-do-for-the-country; *see also* Michael D. Shear et al., *Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers*, N.Y. TIMES, https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html (last updated June 7, 2021).

[67] *See* Osborne, *supra* note 66.

[68] *See* Complaint at 1, EZ Mart 1, LLC v. Colonial Pipeline Co., No. 1:21-cv-02522 (N.D. Ga. filed June 21, 2021); Complaint at 1, Dickerson v. CDCP Colonial Partners, L.P., No. 1:21-cv-02098 (N.D. Ga. filed May 18, 2021).

[69] *See, e.g.*, *North Carolina Gas Station Owner Sues Colonial Pipeline for Losses After Ransomware Attack*, WTVD-TV RALEIGH-DURHAM (June 22, 2021), https://abc11.com/colonial-pipeline-gas-prices-shortage/10821125.

[70] Katie Benner & Nicole Perlroth, *U.S. Seizes Share of Ransom from Hackers in Colonial Pipeline Attack*, N.Y. TIMES (June 7, 2021), https://www.nytimes.com/2021/06/07/us/politics/pipeline-attack.html.

The Justice Department said it seized 63.7 Bitcoins, valued at about $2.3 million (The value of a Bitcoin has dropped over the past month.).[71]

The hack of Colonial Pipeline resulted in a major public policy focus. For example, during May and June 2021, "[President] Biden acted through executive order in an effort to force some . . . [necessary] changes on the pipeline industry, using the Transportation Safety Administration's oversight powers on the pipeline industry."[72]

D. *Kaseya, JBS, and Numerous Others*

Also during mid-2021, information technology firm Kaseya fell victim to a cyberattack on its remote-monitoring and management tool that compromised an estimated "800 to 1500 small to medium-sized companies."[73] Because a "Russia-linked criminal gang" had demanded $70 million (in Bitcoin) from Kaseya for a decryptor,[74] Kaseya took nine days to start restoring customer service.[75] The *New York Times* reported a cyberattack on the world's largest beef supplier (JBS) on June 4, 2021; the attack "was pulled off by a Russian group known as REvil, which has had great success breaking into companies using very simple means . . . email phishing, [by sending] an employee an email that fools him or her into entering a password or clicking on a malicious link."[76] On June 5, 2021, the *Wall Street Journal* reported:

---

[71] *Id.*; *see also* Dustin Volz et al., *U.S. Retrives Million in Ransom Paid to Colonial Pipeline Hacker*, WALL ST. J. (June 7, 2021), https://www.wsj.com/articles/u-s-retrieves-millions-paid-to-colonial-pipeline-hackers-11623094399.

[72] David E. Sanger & Nicole Perlroth, *White House Warns Companies to Act Now on Ransomware Defenses*, N.Y. TIMES (June 4, 2021), https://www.nytimes.com/2021/06/03/us/politics/ransomware-cybersecurity-infrastructure.html.

[73] Charlie Osborne, *Updated Kaseya Ransomware Attack FAQ: What We Know Now*, ZDNET (July 23, 2021, 5:33 AM), https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now.

[74] Ryan Gallagher & Andrew Martin, *Kaseya Failed to Address Security Before Hack, Ex-Employees Say*, BLOOMBERG (July 10, 2021, 8:00 AM), https://www.bloomberg.com/news/articles/2021-07-10/kaseya-failed-to-address-security-before-hack-ex-employees-say.

[75] *Updates Regarding VSA Security Incident*, KASEYA, https://www.kaseya.com/potential-attack-on-kaseya-vsa (last visited Mar. 5, 2024).

[76] Sanger & Perlroth, *supra* note 72.

> FBI Director Christopher Wray said the agency was investigating about 100 different types of ransomware, many tracing back to hackers in Russia, and compared the current spate of cyberattacks with the challenge posed by the Sept. 11, 2001, terrorist attack. . . .
>
> Complaints to the FBI and reports from the private sector show ransomware incidents have tripled in the past year, Mr. Wray said. While private-sector estimates of the toll to the U.S. economy vary, companies that track ransomware generally put the cost at hundreds of millions or billions of dollars annually and say it is rapidly increasing.[77]

Space limitations preclude the mentioning of additional ransomware attacks here, given that 65,000 successful attacks are estimated to have taken place during 2020 alone.[78] However, for those desiring additional information about ransomware attacks, additional sources are footnoted in this Article.[79]

---

[77] Aruna Viswanatha & Dustin Volz, *FBI Director Compares Ransomware Challenge to 9/11*, WALL ST. J. (June 4, 2021, 12:56 PM), https://www.wsj.com/articles/fbi-director-compares-ransomware-challenge-to-9-11-11622799003.

[78] Sanger & Perlroth, *supra* note 72.

[79] *See* Christine Abely, *Ransomware, Cyber Sanctions, and the Problem of Timing*, 63 B.C. L. REV. E.SUPP. I.-47, I.-47 (2022); Micheline Al Harrack, *The Bitcoin Heist: Classifications of Ransomware Crime Families*, 13 INT'L J. COMP. SCI. & INFO. TECH. 75, 75 (2021); Terrence August et al., *Economics of Ransomware: Risk Interdependence and Large-Scale Attacks*, 68 MGMT. SCI. 8979, 8979 (2022); RODERIC BROADHURST ET AL., CYBER TERRORISM: RESEARCH REVIEW iii–v (2017), https://ssrn.com/abstract=2984101; Zen Chang, *Cyberwarfare and International Humanitarian Law*, 9 CREIGHTON INT'L & COMP. L.J. 29, 29 (2017); Lin Cong et al., An Anatomy of Crypto-Enabled Cybercrimes 5 (May 25, 2023), https://ssrn.com/abstract=4188661; Deven R. Desai & Christos Makridis, Identifying Critical Infrastructure in a World with Network Cybersecurity Risk (Sept. 16, 2020), https://ssrn.com/abstract=3693544; Kristen Eichensehr, *Giving Up on Cybersecurity*, 64 UCLA L. REV. DISC. 320, 320 (2016); JULIO HERNANDEZ-CASTRO ET AL., ECONOMIC ANALYSIS OF RANSOMWARE 1 (2017), https://ssrn.com/abstract=2937641; Janine Hiller et al., Strategies for Boosting Cybersecurity 4, 6 (June 1, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4132506; Ido Kilovaty, *Availability's Law*, 88 TENN. L. REV. 69, 71 (2020); Asaf Lubin, *The Law and Politics of Ransomware*, 55 VAND. J. TRANSNAT'L L. 1177, 1179 (2022); Edward A. Morse & Ian Ramsey, *Navigating*

E. *SolarWinds*

The SolarWinds 2020 hack infiltrated over 18,000 government and private networks.[80] As an example of what an initial corporate disclosure of an actual major breach looks like, on December 14, 2020, Austin, Texas–based SolarWinds Corporation issued the following report, as filed with the SEC on Form 8-K, stating:

> SolarWinds Corporation ("SolarWinds" or the "Company") has been made aware of a cyberattack that inserted a vulnerability within its Orion monitoring products which, if present and activated, could potentially allow an attacker to compromise the server on which the Orion products run. SolarWinds has been advised that this incident was likely the result of a highly sophisticated, targeted and manual supply chain attack by an outside nation-state, but SolarWinds has not independently verified the identity of the attacker.[81]

Just three months later, as SolarWinds filed its next annual report, the disclosed "risk factors" language contained the following statement:

---

the Perils of Ransomware, 72 BUS. LAW. 287, 288 (2017); Scott J. Shackelford, *Wargames: Analyzing the Act of War Exclusion in Cyber Risk Insurance Coverage and Its Implications for Cybersecurity Policy*, 23 YALE J.L. & TECH. 362, 369–70 (2021); Jason E. Thomas & Gordon C. Galligher, *Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware*, 11 COMPUT. & INFO. SCI. 14, 15 (2018); Amy Deen Westbrook, *A Safe Harbor for Ransomware Payments: Protecting Stakeholders, Hardening Targets, and Defending National Security*, 18 N.Y.U. J.L. & BUS. 391, 401 (2022).

[80] Steven Vaughan-Nichols, *SolarWinds: The More We Learn, the Worse It Looks*, ZDNET (Jan. 4, 2021, 12:35 PM), https://www.zdnet.com/article/solarwinds-the-more-we-learn-the-worse-it-looks; *see also* Tabrez Y. Ebrahim, *National Cybersecurity Innovation*, 123 W. VA. L. REV. 483, 485 (2020) ("Following Stuxnet, in 2012, U.S. Secretary of Defense Leon Panetta warned that the U.S. was vulnerable to a 'cyber Pearl Harbor . . . .'") (citing SEAN T. LAWSON, CYBERSECURITY DISCOURSE IN THE UNITED STATES 1918, 1953 (Taylor & Francis ed. 2019)); Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. & POL'Y 341, 347 (2015).

[81] SolarWinds Co., Current Report (Form 8-K), at Item 8.01 (Dec. 14, 2020).

> Cyberattacks, including the Cyber Incident, and other security incidents have resulted, and in the future may result, in compromises or breaches of our and our customers' systems, the insertion of malicious code, malware, ransomware or other vulnerabilities into our systems and products and in our customers' systems, the exploitation of vulnerabilities in our and our customers' environments, theft or misappropriation of our and our customers' proprietary and confidential information, interference with our and our customers' operations, expose us to legal and other liabilities, result in higher customer, employee and partner attrition and the loss of key personnel, negatively impact our sales, renewals and upgrade and expose us to reputational harm and other serious negative consequences, any or all of which could materially harm our business.
>
> The Cyber Incident has and is likely to continue to have an adverse effect on our business, reputation, customer, employee and partner relations, results of operations, financial condition or cash flows.[82]

University of Texas at Austin Professor and Associate Dean Robert M. Chesney provides an excellent description of the SolarWinds case within the main text used in his interdisciplinary course attended by students from the UT "schools of law, public affairs, computer science, engineering, communications, and business."[83] Professor Chesney writes:

> SolarWinds specializes in network-management tools—that is, software that large enterprises use to monitor and control conditions throughout their information technology environment. Its products are in widespread use around the world, including a wide

---

[82] SolarWinds Co., Annual Report (Form 10-K), at Item 1A (Mar. 1, 2021).

[83] ROBERT M. CHESNEY, CHESNEY ON CYBERSECURITY LAW, POLICY, AND INSTITUTIONS 1, 4 (3d ed. 2021) (ebook).

> array of prominent private sector entities and government agencies. Among its most successful products is a network monitoring system called Orion. . . .
>
> What follows is a detailed account of the complex sequence of operations SVR conducted as part of the Holiday Bear campaign. As we shall see, exploiting SolarWinds was a central part of the campaign, but there is far more to the story than that (indeed, the intense media focus on SolarWinds has had the unfortunate effect of deflecting attention from the shortcomings of other companies and government agencies).
>
> **Step one: accessing the SolarWinds "build environment"** It is one thing to recognize that SolarWinds customers might not detect a trojaned Orion update, but quite another to compromise the update system in the first place. . . .
>
> **Step two: injecting malware into an Orion update** SVR's next step was to test drive its access by inserting some innocuous code into the build environment, to see if this could be done without detection. In fall 2019, SVR dipped its toes into the water, inserting a modest batch of innocuous code. It worked; the addition was not detected. Exhibiting remarkable patience, SVR continued with similar experiments for months before at last taking advantage of this access to inject actual malware into an Orion build. It took that step in February 2020.[84]

Rest assured, there is much, much more to the SolarWinds saga.[85] However, we must limit our coverage here due to the limited space allowed for any one journal article. Hopefully, having stimulated your interest to know more, readers will refer to Professor Chesney's text for a deeper account.[86]

---

[84] *Id.* at 4–5.
[85] *See id.*
[86] *Id.*

F. *Cyber Warfare*

In the new, widespread assault on business, Professor Tom C.W. Lin warns:

> State and non-state adversaries are assaulting companies using . . . cyberweapons . . . and restrictions. Instead of military installations and government institutions, private firms are often the preferred targets in this mode of warfare. Instead of soldiers and squadrons with bullets and bombs, the weapons of choice are frequently economic hostilities and cyberattacks.[87]

During the 2022 Russian invasion of Ukraine, "[a]n 'IT army' created by the Ukrainian government urged more than 200,000 followers on its Telegram channel . . . to attempt to take down the website of the Moscow Exchange. Thirty-one minutes later, the channel's administrators shared a screenshot suggesting the exchange's website had been knocked offline."[88] The *New York Times* reported that the Ukrainian war "has provoked an onslaught of cyberattacks by apparent volunteers unlike any that security researchers have seen in previous conflicts, creating widespread disruption, confusion and chaos that researchers fear could provoke more serious attacks by nation-state hackers, escalate the war on the ground or harm civilians."[89] These examples illustrate how the "harsh and complicated realities of business warfare will present some of the most difficult decisions for political leaders, corporate executives, military commanders, legislators, and regulators for the foreseeable future."[90] Professor Lin cautions, "The convergence of global conflicts, private business, and war will have serious lingering legal,

---

[87] Tom C.W. Lin, *Business Warfare*, 63 B.C. L. REV. 1, 2 (2022).

[88] David Uberti, *Hackers Target Key Russian Websites*, WALL ST. J. (Feb. 28, 2022, 4:13 PM), https://www.wsj.com/articles/volunteer-hackers-join-ukraines-fight-against-russia-11646082782.

[89] Kate Conger & Adam Satariano, *Volunteer Hackers Converge on Ukraine Conflict With No One in Charge*, N.Y. TIMES (Mar. 4, 2022), https://www.nytimes.com/2022/03/04/technology/ukraine-russia-hackers.html.

[90] Lin, *supra* note 87, at 63.

economic, and social implications. Contemporary business warfare threatens and impacts every nation, every firm, and every citizen."[91]

A recent example of how these battles are fought by governments and private industry is illustrated by the Russian invasion of Ukraine, where "a few hours before Russian tanks began rolling into Ukraine, alarms went off inside Microsoft's Threat Intelligence Center, warning of a never-before seen piece of 'wiper' malware that appeared aimed at [Ukraine's] government ministries and financial institutions."[92] The *New York Times* reported:

> Within three hours, Microsoft threw itself into the middle of a ground war in Europe—from 5,500 miles away. The threat center, north of Seattle, had been on high alert, and it quickly picked apart the malware, named it "Foxblade" and notified Ukraine's top cyberdefense authority. Within three hours, Microsoft's virus detection systems had been updated to block the code, which erases—"wipes"— data on computers in a network.
>
> Then Tom Burt, the senior Microsoft executive who oversees the company's effort to counter major cyberattacks, contacted Anne Newberger, the White House's deputy national security adviser for cyber- and emerging technologies. Ms. Newberger asked if Microsoft would consider sharing details of the code with the Baltics, Poland, and other European nations, out of fear that the malware would spread Ukraine's

---

[91] *Id.*; *see also* Lawrence J. Trautman et al., *How We Learned to Stop Worrying and Love AI: Analyzing the Rapid Evolution of Generative Pre-Trained Transformer (GPT) and its Impacts on Law, Business, and Society*, 34 ALB. L.J. SCI. & TECH. (forthcoming 2024) (manuscript at 27), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4516154; Lawrence J. Trautman, Sam Altman, OpenAI, and the Importance of Corporate Governance (manuscript at 9–11), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4679613.

[92] David E. Sanger et al., *As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War*, N.Y. TIMES (Feb. 28, 2022), https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html#ThenMicrosoftEnteredtheWar.

> borders, crippling the military alliance or hitting West European banks.[93]

Congressional oversight activities sprang into action, with "[a] bipartisan group of nearly two dozen senators hav[ing] called upon Homeland Security Secretary Alejandro Mayorkas to provide information on any efforts by the Biden administration to protect the United States from potential retaliatory Russian cyber and disinformation threats in the wake of Russia's invasion of Ukraine."[94] The *Wall Street Journal* reported that "the letter—spearheaded by Sens. Jacky Rosen (D., N.V.), a member of the Senate Homeland Security and Governmental Affairs Committee, and Mike Rounds (R., S.D.), ranking member of the Senate Armed Services subcommittee on cybersecurity—also requested a briefing from the Department of Homeland Security . . . ."[95] The senators also "questioned what, if any, strategy exists to protect U.S. critical infrastructure from being targeted should Moscow respond to the global crackdown. They also requested information on what the U.S. is doing to defend against Russian disinformation efforts, including whether that threat level has changed."[96]

II. EVOLUTION OF CYBERSECURITY LEGAL LANDSCAPE

A. *Overview of Sources of Cybersecurity Legal Authority*

In 1993, in the wake of the World Trade Center Bombing and the bombing of the Alfred P. Murrah Federal Building in Oklahoma

---

93 *Id.*

94 Vivian Salama, *Senators Request DHS Briefing on Efforts to Protect U.S. From Russian Cyberattacks, Propaganda*, WALL ST. J. (Mar. 14, 2022, 10:19 AM), https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-14/card/senators-request-dhs-briefing-on-efforts-to-protect-u-s-from-russian-cyberattacks-propaganda-d5eFRPIsG78jxTKeE3A0.

95 *Id.*

96 *Id.*

City,[97] Congress enacted the Antiterrorism and Effective Death Penalty Act of 1996 ("AEDPA").[98] AEDPA is a generalized statute that aided the government's ability to prosecute terrorists.[99] It has been argued that some major ransomware gangs operating outside of the United States could qualify as Foreign Terrorist Organizations ("FTOs"), and their attacks qualify as terrorism under AEDPA.[100] However, it was the terrorist attack on America—the destruction of the World Trade Center in New York City; attack on the Pentagon; and loss of United Airlines Flight 93 over Somerset County, Pennsylvania, on September 11, 2001—that resulted in emergency focus on specific cybersecurity legislation.[101] Accordingly, we now present a brief chronological overview of the development of U.S. cybersecurity legal authority, the focus starting with the Oklahoma City bombing leading to the PDD63 in 1999.

B. *Federal Statutes and Regulations*

As early as the mid-1990s, the "growing threat of international terrorism" led policymakers to "reconsider the definition of 'infrastructure' in the context of homeland security."[102] During 1996, President Clinton recognized that:

> These critical infrastructures include telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire and rescue), and conti-

---

[97] Chris Laughlin, *Cybersecurity in Critical Infrastructure Sectors: A Proactive Approach to Ensure Inevitable Laws and Regulations Are Effective*, 14 COLO. TECH. L.J. 345, 346 (2016).

[98] *See generally* Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, 110 Stat. 1214 (codified as amended in scattered sections of 8, 15, 18, 22. 28. 40, 42, 50 U.S.C.).

[99] Laughlin, *supra* note 97, at 346.

[100] Jake C. Porath, *Typing a Terrorist Attack: Using Tools from the War on Terror to Fight the War on Ransomware*, 50 PEPP. L. REV. 139, 147 (2023).

[101] *See* Stuart S. Malawer, *Global Law and Global Challenges*, 58 VA. LAW. 27, 27 (2010).

[102] JOHN MOTEFF & PAUL PARFOMAK, CONG. RSCH. SERV., RL32631, CRITICAL INFRASTRUCTURE AND KEY ASSETS: DEFINITION AND IDENTIFICATION 3 (2004).

> nuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats").[103]

In October 2001, Executive Order 13228[104] created the Office of Homeland Security and required the protection of:

> 1. Energy production, transmission, and distribution services and critical facilities;
>
> 2. Other utilities;
>
> 3. Telecommunications;
>
> 4. Facilities that produce, use, store, or dispose of nuclear material;
>
> 5. Public and privately owned information systems;
>
> 6. Special events of national significance;
>
> 7. Transportation, including railways, highways, shipping ports and waterways;
>
> 8. Airports and civilian aircraft; and
>
> 9. Livestock, agriculture, and systems for the provision of water and food for human use and consumption.[105]

An additional 2001 executive order, Executive Order 13231, created President Bush's Critical Infrastructure Protection Board.[106] A definition of "critical infrastructure" appears in the USA

---

[103] Exec. Order No. 13,010, 61 Fed. Reg. 37,347 (July 15, 1996).

[104] Exec. Order No. 13,228, 66 Fed. Reg. 51,812 (Oct. 8, 2001).

[105] *See* MOTEFF & PARFOMAK, *supra* note 102, at 6 (citing Exec. Order No. 13,228, *supra* note 104).

[106] *Id.* (citing Exec. Order No. 13,231, 66 Fed. Reg. 53,063 (Oct. 16, 2001)).

PATRIOT Act of 2001 (P.L. 107-56),[107] and the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* outlines the Bush Administration's strategy for homeland security. [108] Despite the alarming growth in cyber breaches, more fully discussed *infra*,[109] it wasn't until many years later that Congress acted.[110]

C. *Critical Infrastructure and Executive Order 13636*

During 2012, Senate Bill S.2105 (Cybersecurity Act of 2012), also known as the Lieberman Cybersecurity Act, which required private companies operating critical infrastructure to meet certain security requirements, was defeated in the Senate.[111] This proposal required companies operating "power plants, oil pipelines and other vital services to meet certain security standards."[112] Other requirements included establishing a "mechanism for industry to more easily share information on threats with the government."[113] As a result, The White House started circulating a draft cybersecurity executive order that "would establish a voluntary program where companies operating critical infrastructure would elect to meet cyber security best practices and standards crafted, in part, by the government."[114]

---

[107] *See* MOTEFF & PARFOMAK, *supra* note 102, at 6–7.

[108] *See* GEORGE W. BUSH, EXEC. OFF. OF THE PRESIDENT, THE NATIONAL STRATEGY FOR THE PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURES AND KEY ASSETS vii, 3–4 (2003).

[109] *See infra* Part I.

[110] *See* Lawrence J. Trautman, *Managing Cyberthreat*, 33 SANTA CLARA HIGH TECH. L.J. 230, 254 (2017).

[111] Cybersecurity Act of 2012, S. 2105, 112th Cong. § 104 (2012).

[112] *See* Siobhan Gorman, *Senators Push Bill on Digital Security*, WALL ST. J. (Feb. 15, 2012), https://www.wsj.com/articles/SB10001424052970204062704577223691540531940; Stephen Dycus, *Congress's Role in Cyber Warfare*, 4 J. NAT'L SEC. L. & POL'Y 155, 165 (2010); Lawrence J. Trautman, *Is Cyberattack The Next Pearl Harbor?*, 18 N.C. J.L. & TECH. 233, 235–36 (2016) (describing what a potential massive cyberattack on U.S. critical infrastructure might look like).

[113] Gorman, *supra* note 112.

[114] Jennifer Martinez, *White House Circulating Draft of Executive Order on Cybersecurity*, HILL (Sept. 6, 2012, 11:56 PM), http://thehill.com/blogs/hillicon-valley/technology/248079-white-house-circulating-draft-of-executive-order-on-cybersecurity; *see also* Siobhan Gorman, *Senator Presses on Cybersecurity*, WALL ST. J., (Sept. 19, 2012, 12:03 AM), https://www.wsj.com/articles/SB10000872396390443720204578004690006299614.

President Obama signed Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013, which directs the Executive Branch to:

> 1. Develop a technology-neutral voluntary cybersecurity framework;
>
> 2. Promote and incentivize the adoption of cybersecurity practices;
>
> 3. Increase the volume, timeliness and quality of cyber threat information sharing;
>
> 4. Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure; and
>
> 5. Explore the use of existing regulation to promote cyber security.[115]

In addition, Presidential Policy Directive-21: Critical Infrastructure Security and Resilience replaces Homeland Security Presidential Directive-7 and directs the Executive Branch to:

> 1. Develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time;
>
> 2. Understand the cascading consequences of infrastructure failures;
>
> 3. Evaluate and mature the public-private partnership;
>
> 4. Update the National Infrastructure Protection Plan; and
>
> 5. Develop comprehensive research and development plan.[116]

---

[115] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013).

[116] U.S. DEP'T OF HOMELAND SEC., EXECUTIVE ORDER (EO) 13636 IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY: PRESIDENTIAL POLICY

The 2013 Executive Order (Executive Order 13636) provides a definition of the term "critical infrastructure" to mean "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[117] Executive Order 13636 also directs "the Secretary of the Treasury, along with the Secretary of Commerce and the Secretary of Homeland Security to each make recommendations on a set of incentives that would promote private sector participation in the voluntary program."[118] Perhaps the most significant contribution of Executive Order 13636 is that it mandates "development of a voluntary risk-based Cybersecurity Framework—a set of industry standards and best practices to help organizations manage cybersecurity risks. [This] resulting Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk."[119] In retrospect, a major benefit derived from the Framework is that it provides an organic template for establishment and growth of an organization's cybersecurity program.

DIRECTIVE (PPD)-21 CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (2013), https://www.cisa.gov/sites/default/files/publications/eo-13636-ppd-21-fact-sheet-508.pdf.

[117] Exec. Order No. 13,636, *supra* note 115.

[118] U.S. DEP'T OF TREASURY DEP'T, TREASURY DEPARTMENT REPORT TO THE PRESIDENT ON CYBERSECURITY INCENTIVES PURSUANT TO EXECUTIVE ORDER 13636, 2–3 (2013) ("The Secretary of [Homeland Security] shall coordinate establishment of a set of incentives designed to promote participation in the [voluntary cybersecurity] Program. Within 120 days of the date of this order, the Secretary and Secretaries of the Treasury and Commerce each shall make recommendations separately to the President, through the Assistant to the President for Homeland Security and Counterterrorism and the Assistant to the President for Economic Affairs, that shall include analysis of the benefits and relative effectiveness of such incentives, and whether the incentives would require legislation or can be provided under existing law or authorities to participants in the Program." (quoting Exec. Order No. 13,636, *supra* note 115)).

[119] *See* NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY: VERSION 1.0, 1 (2014); *see also* Scott Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 308–09 (2015).

D. *Legislative Action: 113th Congress*

Despite the fact that Congress had held hearings on the topic of cybersecurity during every year since 2001, it wasn't until December 18, 2014, that comprehensive cybersecurity legislation was signed into law in the form of five new statutes:

> 1. The Cybersecurity Workforce Assessment Act, which requires the DHS to develop a cyber-workforce strategy;[120]
>
> 2. The Cybersecurity Enhancement Act of 2014, which codifies the National Institute of Standards and Technology's (NIST's) role in cybersecurity;[121]
>
> 3. The Border Patrol Agent Pay Reform Act of 2014, which gives DHS new authorities for cybersecurity hiring;[122]
>
> 4. The National Cybersecurity Protection Act of 2014, which codifies DHS's cybersecurity center;[123] and
>
> 5. The Federal Information Security Modernization Act of 2014, which Reforms federal IT security management.[124]

E. *Legislative Action: 114th Congress*

H.R. 2029, the Consolidated Appropriations Act, was signed into law on December 18, 2015; it represented a compromise between the House Homeland Security Committee and the House and

---

[120] Cybersecurity Workforce Assessment Act, 6 U.S.C. § 146.

[121] Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 2971 (codified as amended in scattered sections of 15 U.S.C.).

[122] Border Patrol Agent Pay Reform Act of 2014, Pub. L. No. 113-277, 128 Stat. 2995 (codified as amended in scattered sections of 5 U.S.C. and 6 U.S.C.).

[123] National Cybersecurity Protection Act of 2014, Pub. L. No. 113-282, 128 Stat. 3066 (codified as amended in scattered sections of 6 U.S.C.).

[124] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (codified as amended in scattered sections of 44 U.S.C.).

Senate Intelligence Committees.[125] The omnibus law's cybersecurity provisions "are located in Division N (Cybersecurity Act of 2015), including Title I, Cybersecurity Information Sharing; Title II, National Cybersecurity Advancement; Title III, Federal Cybersecurity Workforce Assessment; and Title IV, Other Cyber Matters."[126]

F. *Federal Executive Orders, 2016–2020*

President Obama issued Executive Order 13691 in February 2015; it was designed to facilitate cybersecurity information sharing among entities in the private sector.[127] Two significant executive order and presidential directive developments impacting U.S. cybersecurity policy took place on December 29, 2016. The first of these developments was Executive Order 13757, *Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities*:

> This amends Executive Order 13694, 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,' which authorized the imposition of sanctions on individuals and entities determined to be responsible for or complicit in malicious cyber-enabled activities that result in enumerated harms that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States. The authority has been amended to allow for the imposition of sanctions on individuals and entities determined to be responsible for tampering, altering, or causing the misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions.

---

[125] *See* Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, 129 Stat. 2242 (2015); *see also* RITA TEHAN, CONG. RSCH. SERV., R43317, CYBERSECURITY: LEGISLATION, HEARINGS, AND EXECUTIVE BRANCH DOCUMENTS 3 (2017).

[126] TEHAN, *supra* note 125, at 3.

[127] *See* Exec. Order No. 13,691, 80 Fed. Reg. 9,349 (Feb. 13, 2015) (promoting information sharing and analysis organizations (ISAOs) as defined in the Homeland Securities Act (6 U.S.C. § 131 (5))).

> Five entities and four individuals are identified in the Annex of the amended executive order and will be added to the Office of Foreign Assets Control's (OFAC's) list of Specially Designated Nationals and Blocked Persons (SDN List).[128]

The next significant cybersecurity policy development to take place on December 29, 2016, was an Amended Executive Order 13694, *Cyber-Related Sanctions Designations*, which:

> Authorizes the imposition of sanctions on individuals and entities determined to be responsible for or complicit in malicious cyber-enabled activities that result in enumerated harms that are reasonably likely to result in, or have materially contributed to, a significant threat to the national security, foreign policy, or economic health or financial stability of the United States. The authority has been amended to also allow for the imposition of sanctions on individuals and entities determined to be responsible for tampering, altering, or causing the misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions. Five entities and four individuals are identified in the Annex of the amended Executive Order and will be added to OFAC's list of Specially Designated Nationals and Blocked Persons (SDN List). OFAC today is designating an additional two individuals who also will be added to the SDN List.[129]

Other 2016 developments included the Presidential Policy Directive 41, *United States Cyber Incident Coordination*, issued July 26, 2016, which:

> [S]ets forth principles governing the federal government's response to any cyber incident, whether involving government or private-sector entities. For significant cyber incidents, the PPD establishes lead

---

128 TEHAN, *supra* note 125, at 45–46.

129 *Id.* at 45.

> federal agencies and architecture for coordinating the broader federal government response. The PPD also requires the Departments of Justice and Homeland Security to maintain updated contact information for public use to assist entities affected by cyber incidents in reporting those incidents to the proper authorities.[130]

Worthy of mention here is Executive Order 13718, issued on February 9, 2016, which established a Commission on Enhancing National Cybersecurity comprised "of 12 members appointed by the President, including 'top strategic, business, and technical thinkers from outside of Government—including members to be designated by the bi-partisan Congressional leadership.'"[131] In addition, Executive Order 13694, *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities*, was issued April 1, 2015, providing for:

> [T]he first sanctions program to allow the Administration to impose penalties on individuals overseas who engage in destructive attacks or commercial espionage in cyberspace. The order declares 'significant malicious cyber-enabled activities' a 'national emergency' and enables the Treasury Secretary to target foreign individuals and entities that take part in the illicit cyberactivity for sanctions that could include freezing their financial assets and barring commercial transactions with them.[132]

On May 11, 2017, President Trump issued an executive order entitled "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure."[133] This Executive Order "requires an assessment of cybersecurity risks at every agency, orders a review of cur-

---

130 *Id.* at 46.
131 *Id.*
132 *Id.* at 46–47.
133 Exec. Order No. 13,800, 82 Fed. Reg. 22,391 (May 11, 2017).

rent efforts to protect vital infrastructure like power plants and hospitals, and requires a report on building the cybersecurity workforce."[134]

G. *2023 Quadrennial Homeland Security Reviews*

In April 2023, the 2023 Quadrennial Homeland Security Review reaffirmed "the five enduring homeland security missions articulated in the first two QHSR Reports issued in 2010 and 2014," and focused on "how the Department must adapt and evolve to accomplish them."[135] The DHS report warned, "Today, the most significant terrorist threat stems from lone offenders and small groups of individuals, especially domestic violent extremists, while the threat of international terrorism remains as foreign terrorist organizations have proven adaptable and resilient . . . [and] have continued to launch attacks in their names."[136]

H. *U.S. Comprehensive Federal Digital Assets Strategy*

On March 9, 2022, President Biden signed an Executive Order providing for the first-ever comprehensive federal digital assets strategy, to assist the U.S. in "playing a leading role in the innovation and governance of the digital assets ecosystem at home and abroad, in a way that protects consumers, is consistent with our democratic values and advances U.S. global competitiveness."[137] The Executive Order stated that "growing development and adoption of digital assets and related innovations, as well as inconsistent controls to defend against certain key risks, necessitate an evolution and alignment of the United States Government approach to digital assets."[138] Accordingly, it:

---

[134] TEHAN, *supra* note 125, at 45.

[135] Letter from Alejandro N. Mayorkas, Sec'y of Homeland Sec., *in* U.S. DEP'T OF HOMELAND SEC., THE THIRD QUADRENNIAL HOMELAND SECURITY REVIEW (2023).

[136] *Id.*

[137] Press Release, White House, Statement by NEC Director Brian Deese and National Security Advisor Jake Sullivan on New Digital Assets Executive Order (Mar. 9, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/09/statement-by-nec-director-brian-deese-and-national-security-advisor-jake-sullivan-on-new-digital-assets-executive-order.

[138] Exec. Order No. 14,067, 87 Fed. Reg. 14,143 (Mar. 9, 2022).

> Advances in digital and distributed ledger technology for financial services have led to dramatic growth in markets for digital assets, with profound implications for the protection of consumers, investors, and businesses, including data privacy and security; financial stability and systemic risk; crime; national security; the ability to exercise human rights; financial inclusion and equity; and energy demand and climate change. In November 2021, non-state issued digital assets reached a combined market capitalization of $3 trillion, up from approximately $14 billion in early November 2016. Monetary authorities globally are also exploring, and in some cases introducing, central bank digital currencies (CBDCs) . . . .
>
> The United States has an interest in responsible financial innovation, expanding access to safe and affordable financial services, and reducing the cost of domestic and cross-border funds transfers and payments, including through the continued modernization of public payment systems. We must take strong steps to reduce the risks that digital assets could pose to consumers, investors, and business protections; financial stability and financial system integrity; combating and preventing crime and illicit finance; national security; the ability to exercise human rights; financial inclusion and equity; and climate change and pollution.[139]

The Executive Order calls for a report to be submitted to the President within 180 days about payment systems and the future of money, including "the conditions that drive broad adoption of digital assets; the extent to which technological innovation may influence these outcomes; and the implications for the United States financial system, the modernization of and changes to payment sys-

---

[139] *Id.*

tems, economic growth, financial inclusion, and national security."[140] The following digital asset policy objectives are outlined in the Executive Order:

> (a) We must protect consumers, investors, and businesses in the United States;
>
> (b) We must protect United States and global financial stability and mitigate systemic risk;
>
> (c) We must mitigate the illicit finance and national security risks posed by misuse of digital assets;
>
> (d) We must reinforce United States leadership in the global financial system and in technological and economic competitiveness, including through the responsible development of payment innovations and digital assets;
>
> (e) We must promote access to safe and affordable financial services; and
>
> (f) We must support technological advances that promote responsible development and use of digital assets.[141]

I. *Executive Order 14028, Improving the Nation's Cybersecurity*

On May 12, 2021, Executive Order 14028, *Improving the Nation's Cybersecurity*, was issued; the order "focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development environments."[142] The order directs agencies "to take a variety of actions that 'enhance the

---

[140] *Id.* at 14146.

[141] *Id.* at 14143–45.

[142] SHALANDA D. YOUNG, OFF. OF MGMT. & BUDGET, EXEC. OFF. OF THE PRESIDENT, MEMORANDUM NO. M-23-16, UPDATE TO MEMORANDUM M-22-18: ENHANCING THE SECURITY OF THE SOFTWARE SUPPLY CHAIN THROUGH SECURE SOFTWARE DEVELOPMENT PRACTICES (2023).

security of the software supply chain.'"[143] In accordance with Executive Order 14028, the "National Institute of Standards and Technology ('NIST') has released the NIST Secure Software Development Framework ('SSDF'), SP 800218, and the NIST Software Supply Chain Security Guidance."[144]

J. *National Security Memorandum 8 (NSM-8)*

As a follow-up to Executive Order 14028, National Security Memorandum 8 (NSM-8) addresses cybersecurity requirements for those national security areas of the Federal Information systems and "establishes methods to secure exceptions for circumstances necessitated by unique mission needs."[145]

K. *National Security Memorandum 10 (NSM-10)*

On May 4, 2022, President Biden issued National Security Memorandum 10 (NSM-10), *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems*.[146] This directive outlines President Biden's "policies and initiatives related to quantum computing."[147] The Memorandum "identifies key steps needed to maintain the Nation's competitive advantage in quantum information science (QIS), while mitigating the risks of quantum computers to the Nation's cyber, economic, and national security."[148] Readers interested in this topic should also see the *NIST Post-Quantum Cryptography Standardization*[149] and *NSM-10*.[150]

---

143 *Id.*

144 *Id.*

145 Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, 2022 DAILY COMP. PRES. DOC. 1 (Jan. 19, 2022).

146 Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, 2022 DAILY COMP. PRES. DOC. 1 (May 4, 2022).

147 *Id.*

148 *Id.*

149 *Post-Quantum Cryptography Standardization*, NIST (Jan. 11, 2024), https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization.

150 Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems, 2022 DAILY COMP. PRES. DOC. 1 (Jan. 19, 2022).

III. CYBERSECURITY AND CORPORATE GOVERNANCE

For many years, U.S. law has recognized two primary standards for the conduct of corporate directors: duties of loyalty and care. These aspects of corporate governance have become increasingly important given the governance gaps in federal cybersecurity policy described in Part II.

A. *Duty of Loyalty*

The common law fiduciary duty of loyalty requires a corporate director to use good faith in the oversight of a corporation.[151] *In re Caremark*[152] and subsequent cases established that a director's oversight responsibilities are included in the duty of loyalty.[153] To satisfy the duty of loyalty, a director must "make a good faith effort to implement an oversight system and then monitor it."[154] This oversight requires oversight and reporting of a corporation's "central compliance risks."[155] These risks likely would include cybersecurity breaches.

B. *Duty of Care*

Professors Trautman and Ormerod have previously written that "the duty of care is a concept adapted from tort law, and it requires an actor to behave reasonably."[156] As a threshold matter, "[d]irector liability for a breach of the duty of care may, in theory, arise in two distinct contexts."[157] First, liability may "follow *from a board decision* that results in a loss because that decision was ill advised or

---

[151] Anne Tucker Nees, *Who's the Boss? Unmasking Oversight Liability Within the Corporate Power Puzzle*, 35 DEL. J. CORP. L. 199, 204 (2010).

[152] *See In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 972 (Del. Ch. 1996).

[153] Alberto R. Salazar V., *Implementing the New Purpose of the Corporation: The Duty of Directors to Tie Executive Pay to Employees' Interests*, 20 BERKELEY BUS. L.J. 149, 161 (2023).

[154] Marchand v. Barnhill, 212 A.3d 805, 821 (Del. 2019).

[155] *Id.* at 824.

[156] Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach*, 66 AM. U. L. REV. 1231, 1245 (2017) (citing Robert J. Rhee, *The Tort Foundation of Duty of Care and Business Judgment*, 88 NOTRE DAME L. REV. 1139, 1141, 1159–60 (2013)).

[157] *In re Caremark*, 698 A.2d at 967.

'negligent.'"[158] Second, director liability may "arise from an unconsidered failure of the board to act in circumstances in which due attention would, arguably, have prevented the loss."[159]

C. *Duty to Monitor*

A breach of the duty to monitor arises when "a loss eventuates not from a decision but, from unconsidered inaction."[160] Observing that "most of the decisions that a corporation, acting through its human agents, makes are . . . not the subject of director attention," the court in *Caremark* nonetheless recognized that "ordinary business decisions that are made by officers and employees deeper in the interior of the organization can . . . vitally affect the welfare of the corporation and its ability to achieve its various strategic and financial goals."[161] The obligation to be reasonably informed requires that corporate boards at a minimum must "assur[e] themselves that information and reporting systems exist in the organization that are reasonably designed to provide . . . timely, accurate information sufficient to allow management and the board . . . to reach informed judgments concerning . . . the corporation's compliance with law."[162]

In a cybersecurity context, the duty to monitor requires "the board [to] exercise a good faith judgment that the corporation's information and reporting system is in *concept and design* adequate to assure the board that appropriate information will come to its attention in a timely manner."[163] Therefore, to avoid liability and conform to relevant legal norms, directors should make a good faith attempt to ensure the company has a "corporate information and reporting system" that the board finds satisfactory.[164] In summary, the corporate law duty of care centers on whether corporate directors

---

158 *Id.*

159 *Id.* (emphasis omitted) (citing E. Norman Veasey & Julie M.S. Seitz, *The Business Judgment Rule in the Revised Model Act, the* Trans Union *Case, and the ALI Project—A Strange Porridge*, 63 TEX. L. REV. 1483, 1493 (1985)).

160 *Id.* at 968.

161 *Id.*

162 *Id.* at 970.

163 *In re Caremark*, 698 A.2d at 970 (emphasis added).

164 *Id.* at 970.

and officers employed a "good faith effort" to remain reasonably informed in order to "exercise appropriate judgment."[165]

D. *Duty to Disclose*

Publicly traded corporations have a duty to disclose the existence of a data breach based upon at least two distinct authorities: Delaware state corporate common law and the SEC's 2011 corporate finance disclosure guidance, which identifies material data security risks that companies must disclose under securities law disclosure requirements and accounting standards.[166] Accordingly, companies that know about a data breach but fail to disclose it to shareholders, regulators, and consumers potentially risk liability under corporate, breach notification, and securities laws.

The concept that directors and officers of a corporation have a fiduciary duty of disclosure to shareholders and the corporation, sometimes referred to as a duty of complete candor, is well established in Delaware common law.[167] Many years ago, Professor Lawrence A. Hamermesh noted that Delaware courts have recognized "that a fiduciary duty to disclose all material information arises when directors approve any public statement, such as a press release, regardless of whether any specific stockholder action is sought."[168]

---

[165] *Id.* at 968; *see also* Christopher M. Bruner, *Is the Corporate Director's Duty of Care a "Fiduciary" Duty? Does It Matter?*, 48 WAKE FOREST L. REV. 1027, 1031, 1047 (2013) (asserting that liability under the *Caremark* standard requires bad intention toward the company, such as "total board failure to engage in oversight"); William T. Allen et al., *Realigning the Standard of Review of Director Due Care with Delaware Public Policy: A Critique of* Van Gorkom *and Its Progeny as a Standard of Review Problem*, 96 NW. U. L. REV. 449, 457 n.31 (2002) (stating that directors "will not be held liable" for a breach of the duty to monitor without a finding of bad faith); Lynn A. Stout, *In Praise of Procedure: An Economic and Behavioral Defense of* Smith v. Van Gorkom *and the Business Judgment Rule*, 96 NW. U. L. REV. 675, 680 (2002) (noting that in some states, directors are presumed to meet the duty of care if the decision was "informed," and "unless the directors [have been] *grossly* negligent in failing to inform themselves, before acting," the decision is deemed to be informed).

[166] *See* DIV. OF CORP. FIN., U.S. SEC. & EXCH. COMM'N, CF DISCLOSURE GUIDANCE: TOPIC NO. 2: CYBERSECURITY, Oct. 13, 2011, https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[167] Lawrence A. Hamermesh, *Calling Off the* Lynch *Mob: The Corporate Director's Fiduciary Disclosure Duty*, 49 VAND. L. REV. 1087, 1097 n.36 (1996).

[168] *Id.* at 1091.

E. *Director's Cyber Duty of Care*

Previously, Trautman and Ormerod have provided an economic analysis of steps taken to discharge a director's cybersecurity duty of care.[169] To follow this analysis, please consider Exhibits 6 and 7 presented below.

Exhibit 6 is an illustration of the view Yahoo's senior management appears to have taken.

EXHIBIT 6

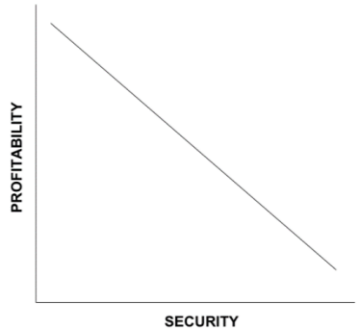
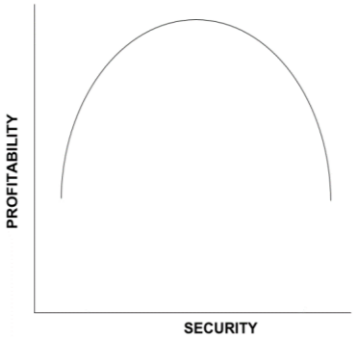


Exhibit 7, on the other hand, we believe is closer to the truth.

EXHIBIT 7



Professors Trautman and Ormerod contend "that viewing the security of companies' electronic features—for technology and non-technology companies alike—as inversely correlated with the usability, and thus the profitability, of those features fails to capture the

[169] Trautman & Ormerod, *supra* note 156, at 1290.

entirety of the complex interplay between security and profitability."[170] Consider that, while Exhibit 6 depicts a fully zero-sum relationship between security and profitability, Exhibit 7 reveals that the inverse relationship between security and profitability is only half the picture (i.e., the right half of the curve).

The relationship depicted in Exhibit 7 may be described like this:

> [A]t the leftmost point on the curve, a company's data security is so abysmal that not only do few, if any, users trust the company with their personal information so as to render the profitability of the company's electronic features a nullity, but also, the prospect of unfavorable judicial determination—e.g., by the FTC—hampers any possibility of profits. Put another way, zero security measures result in zero users, and thus zero profitability. But as the company's security improves, increasing numbers of users trust the company with their personal information and the risk of action by the FTC decreases—both of which contribute to increased profitability. At some point—essentially, where the number of users is maximized—increased security measures begin limiting the usability of the company's electronic features, and thus begin decreasing profitability. Taken to an extreme, excessive security measures may, theoretically, drive usability to point of futility, rendering profit nonexistent. It is important to note that the right half of the curve in [Exhibit 6] is effectively identical to the relationship depicted in [Exhibit 7]: more security means less profit. The critical takeaway is that little or no digital security may be just as damaging to a company's financial health as implementing overly excessive security.[171]

---

170 *Id.* at 1289.

171 *Id.* at 1290–91.

F. Caremark *and Progeny*

Recently, Professors Pace and Trautman have written about several *Caremark* decisions that may significantly impact director liability for cybersecurity governance.[172] For many years now, "Chancellor Allen's description of a *Caremark* claim as possibly the most difficult theory in corporation law upon which a plaintiff might hope to win a judgment held true."[173] For decades, "*Caremark* claims that survived a motion to dismiss were . . . few and far between."[174] However, during 2019, things changed. In just a little over a year, Delaware courts have allowed five *Caremark* claims to survive in the corporation context[175] and one claim to survive in the limited partnership context.[176] Therefore, under what has come to be known as a *Caremark* claim, directors can be held liable for breaching their fiduciary duties to the corporation by failing to provide adequate oversight. *Caremark* claims typically arise where corporate employees caused the corporation to engage in some unlawful conduct and plaintiffs allege that the unlawful conduct would not have taken place had directors acted properly. Conscious disregard "is necessary; *Caremark* is, [therefore], a high bar."[177] Professors Pace and Trautman write:

---

[172] H. Justin Pace & Lawrence J. Trautman, *Mission Critical: Caremark, Blue Bell, and Director Responsibility for Cybersecurity Governance*, 2022 WIS. L. REV. 887, 889 (2022).

[173] *Id.* at 888 (citing *In re* Caremark Int'l Inc. Derivative Litig., 698 A.2d 959, 967 (Del. Ch. 1996)).

[174] *Id.* (citing *In re* China Agritech, Inc. S'holder Derivative Litig., No. 7163-VCL, 2013 WL 2181514, at *1 (Del. Ch. May 21, 2013); Rich *ex rel.* Fuqi Int'l v. Yu Kwai Chong, 66 A.3d 966, 986 (Del. Ch. 2013); *In re* Am. Int'l Grp. Inc., 965 A.2d 763, 831 (Del. Ch. 2009); Saito v. McCall, No. Civ.A. 17132-NC, 2004 WL 3029876, at *11 (Del. Ch. Dec. 20, 2004)).

[175] *Id.* at 889 (citing Marchand v. Barnhill, 212 A.3d 805, 824 (Del. 2019), *reversing* Marchand v. Barnhill, No. 2017-0586-JRS, 2018 WL 4657159 (Del. Ch. Sept. 27, 2018); *In re* The Boeing Co. Derivative Litig., No. 2019-0907-MTZ, 2021 WL 4059934, at *25 (Del. Ch. Sept. 7, 2021); Teamsters Loc. 443 Health Servs. & Ins. Plan v. Chou, No. 2019-0816-SG, 2020 WL 5028065, at *26 (Del. Ch. Aug. 24, 2020); Hughes v. Xiaoming Hu, No. 2019-0112-JTL, 2020 WL 1987029, at *18 (Del. Ch. April 27, 2020); *In re* Clovis Oncology, Inc. Derivative Litig., No. 2017-0222-JRS, 2019 WL 4850188, at *18 (Del. Ch. Oct. 1, 2019)).

[176] *Id.* (citing Inter-Mktg. Grp. U.S., Inc. v. Armstrong, No. 2017-0030-TMR, 2020 WL 756965, at *1 (Del. Ch. Jan. 31, 2020)).

[177] *Id.* ("[T]he concept of *intentional dereliction of duty*, a *conscious disregard for one's responsibilities*, is an appropriate (although not the only) standard for

> The scope and likelihood of *Caremark* liability are matters of considerable interest and concern for directors. Under most circumstances, a board simply doing its job poorly is relevant only to the directors' duty of care and protected by the business judgment rule, exculpatory provisions under Section 102(b)(7),[178] and advancement and indemnification. Failure to monitor under *Caremark*, however, is a breach of the duty of loyalty.[179] A breach of the duty of loyalty is not protected by the business judgment rule. It cannot be exculpated.[180] And it cannot be covered by indemnification.[181]

IV. HOW CORPORATE DIRECTORS GOVERN CYBER THREATS

A. *Evolution of Cyber Corporate Governance*

During 2018, PwC reported, "Many directors are not confident that management has a handle on cyber threats."[182] Drawing on data from PwC's 2017 Annual Corporate Directors Survey, "only 39% of directors are very comfortable that their company has identified

---

determining whether fiduciaries have acted in good faith." (quoting *In re* Walt Disney Co. Derivative Litig., 906 A.2d 27, 62 (Del. 2006))).

[178] Pace & Trautman, *supra* note 172, at 889 (citing DEL. CODE ANN. tit. 8, § 102(b)(7) (2016)).

[179] *Id.* (citing Guttman v. Huang, 823 A.2d 492, 506 (Del. Ch. 2003)).

[180] *Id.* at 890 (citing DEL. CODE ANN. tit. 8, § 102(b)(7)(ii) (2016) ("[T]he certificate of incorporation may also contain . . . [a] provision eliminating or limiting the personal liability of a director to the corporation . . . for monetary damages for breach of fiduciary duty as a director, provided that such provision shall not eliminate or limit the liability of a director: . . . (ii) for acts or omissions not in good faith.")).

[181] *Id.* (citing Hermelin v. K-V Pharm. Co., 54 A.3d 1093, 1111 (Del. Ch. 2012) ("Sections 145(a) and (b) of the DGCL permit a corporation to indemnify [a director] so long as 'the person acted in good faith and in a manner the person reasonably believed to be in or not opposed to the best interests of the corporation, and, with respect to any criminal action or proceeding, had no reasonable cause to believe the person's conduct was unlawful.'") (citing DEL. CODE ANN. tit. 8, § 145(a), (b) (2016)).

[182] Paula Loop et al., *Overseeing Cyber Risk*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Feb. 18, 2018), https://corpgov.law.harvard.edu/2018/02/18/overseeing-cyber-risk.

its most valuable and sensitive digital assets."[183] Then, a year later, "44% of the 9,500 executives surveyed . . . say they don't have an overall information security strategy."[184] When questioned, "In your opinion, which of the following areas of oversight do not receive sufficient board time/attention," and asked to select all that apply among ten choices, the 2021 PwC survey of 851 corporate directors reports that 26% of respondents highlighted cyber/digital/technology.[185] The topic "crisis management" was selected by 29% of those responding.[186] Next, respondents were asked to select only one as an answer to the question, "When your board recruits its next director, what is the single most important attribute your board will prioritize in the search?"[187] As shown in Exhibit 8, "IT/digital expertise" was selected by only 7% of those responding, while "racial/ethnic diversity" led the list with 25%.[188]

EXHIBIT 8

When your board recruits its next director, what is the single most important attribute your board will prioritize in the search?[189]

183 *Id.*

184 *Id.* (citing CHRISTOPHER CASTELLI ET AL., STRENGTHENING DIGITAL SOCIETY AGAINST CYBER SHOCKS 4 (2017)).

185 PWC, THE DIRECTOR'S NEW PLAYBOOK: TAKING ON CHANGE: PWC'S 2021 ANNUAL CORPORATE DIRECTORS SURVEY 25 (2021).

186 *Id.*

187 *Id.* at 22.

188 *Id.* at 22.

189 *Id.*

Given the growing risk and expense of cyber breach, consultant PwC states, "boards recognize the need for an effective cyber risk governance and oversight structure. Such a structure includes the board, IT and management so cyber risks are managed across the company."[190] Although it will likely require time and top leadership commitment to achieve "such a cyber risk management program, the end goal is to have a cost-effective program that addresses the key risks, and allows the company to become cyber resilient."[191] The March 2021 NACD/PwC report, Principles for Board Governance of Cyber Risk, provides additional valuable insight. Exhibit 9 illustrates responses when asked, "What five trends do you foresee having the greatest effect on your company over the next 12 months," 38.9% of those responding listed "changing cybersecurity threats."[192]

EXHIBIT 9

What five trends do you foresee having the greatest effect on your company over the next 12 months?[193]

B. *Governance Challenge of Cyber Resilience*

As early as January 2017, the World Economic Forum, in collaboration with The Boston Consulting Group and Hewlett Packard Enterprise, issued their Future of Digital Economy and Society System Initiative, titled "Advancing Cyber Resilience: Principles and Tools for Boards."[194] Accordingly, the World Economic Forum writes:

---

190 PWC, HOW YOUR BOARD CAN BETTER OVERSEE CYBER RISK 9 (2018).

191 *Id.*

192 LARRY CLINTON ET AL., PRINCIPLES FOR BOARD GOVERNANCE OF CYBER RISK 5 (2021).

193 *Id.*

194 WORLD ECONOMIC FORUM, ADVANCING CYBER RESILIENCE: PRINCIPLES AND TOOLS FOR BOARDS 1 (2017).

> Countering cyber risk presents a significant strategic challenge to leaders across industries and sectors but one that they must surmount in order to take advantage of the opportunities presented by the vast technological advances in networked technology that are currently in their early stages. Over the past decade, we have significantly expanded our understanding of how to build secure and resilient digital networks and connected devices. However, board-level capabilities for strategic thinking and governance in this area have failed to keep pace with both the technological risks and the solutions that new innovations provide.[195]

C. *Directors and Experts Speak About Cyber*

Recently, a group of seasoned corporate directors came together to discuss several contemporary challenges, including cyber-related issues, facing boards.[196] While the executive and board experience credentials far exceed space limitations available here, a few highlights include: Seletha Butler (Truist Bank and St. Joseph's Health System); Michele Hooper (AstraZeneca; PPG Industries; Target Corporation; United Continental Holdings; UnitedHealth Group); Ron McCray (A.H. Belo Corporation; Career Education Corporation; Kimberly-Clark Corporation; Knight-Ridder; Nike, Inc.); Ruth Simmons (Fiat Chrysler; Goldman Sachs; MetLife; Mondelez International; Pfizer; Texas Instruments); and Lawrence Trautman (over thirty corporate boards).[197]

Professor Frederick Chang is a former Director of Research at the National Security Agency (NSA).[198] He is currently the Co-Chair of the Intelligence Community Studies Board of the National Academies of Sciences, Engineering, and Medicine and he is also a member of the Army Research Laboratory Technical Assessment

---

[195] *Id.* at 5.

[196] Lawrence J. Trautman et al., *Corporate Directors: Who They Are, What They Do, Cyber and Other Contemporary Challenges*, 70 BUFF. L. REV. 459, 463 (2022).

[197] *Id.* at 459–60.

[198] *Id.* at 459.

Board of the National Academies.[199] Professor Chang has served as a member of the Computer Science and Telecommunications Board of the National Academies, as a member of the Commission on Cybersecurity for the 44th Presidency, and has appeared before Congress as a cybersecurity expert witness on multiple occasions.[200] Professor Chang warns:

> Basically, what directors need to know about cyber is that it is a strategic risk and not just an IT thing. It's easy to think of it as if, there are some routers or some switches or some firewalls that get broken, resulting in exposed data—creating a problem. It's important to step back and reflect upon how cyber is a risk, like any other risk. It can be thought of like an earthquake, or a flood or a fire. Much like an earthquake, flood or fire—you can't do anything about it if there's going to be an earthquake, and you are located in California. You can't stop the earthquake. All too often, it seems, there is a perception that cyber threat can actually be stopped. It can't be stopped. If a persistent attacker has a really high desire to break through, then they're going to get through. You can't stop them—and cyber has to be viewed as a risk, like any other risk . . . . [T]here are some things you can do to mitigate . . . the risk, but you can't eliminate the risk. Maybe you can buy insurance, you can bring in some more people to work on cybersecurity, and so forth. But cyber threat is fundamentally something you can't stop, and it needs to be viewed at that level. So, what steps does a board take to have enough intrinsic knowledge about cyber? The task can be a highly technical thing, but it isn't only a technical concern.[201]

During this panel discussion, Professor and seasoned corporate director Trautman discusses how, for many years now, boardroom

---

199 *Id.*
200 *Id.*
201 *Id.* at 509–10.

conversation amounts to some version of, "Even if we spend every dollar we could borrow, we still wouldn't have spent enough on cyber. The North Koreans, Russians, Chinese . . . all these nations are engaged in cyber war. We don't have enough money around here to fight a war."[202] Economists refer to this as an externality, where "many boards are just pushing the problem off on the government . . . on their customers . . . [because] there are few prosecutions, because cyber failures are so pervasive . . . because everybody's got the same problem."[203]

D. *Governance by Committee*

Corporate boards organize and conduct their activities by committees.[204] Based on 416 directors reporting, a recent National Association of Corporate Directors survey reports that cybersecurity oversight is conducted primarily at the full board level (44% of directors reporting); audit committee (41%); risk committee (10%); and other (5%).[205] Veteran corporate director Michele Hooper says, "[I]n my experience, my boards have put the cyber oversight role in the audit committee and that's because that's where we're dealing with all things that involve risk."[206] She adds:

> Most of my boards do not have a specific risk committee which tends to be found in finance or insurance type companies, as opposed to other industries.

---

[202] Trautman et al., *supra* note 196, at 513.

[203] *Id.*; *see also* Lawrence J. Trautman, *Is Cyberattack the Next Pearl Harbor?*, 18 N.C. J.L. & TECH. 232 (2016) (exploring the widespread risk by "depict[ing] a fictional scenario of what a cyberattack on a massive scale might look like"); Trautman, *supra* note 110, at 272 (citing a report listing "fragmented responsibilities" as one of the common barriers in organizations that attempt to adopt effective cyber security measures); Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who & How It Works*, 5 J.L. & CYBER WARFARE 147 (2016); Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. & POL'Y 341, 346 (2015) (describing pervasiveness of cybersecurity risk).

[204] Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment*, 11 FLA. ST. U. BUS. REV. 75, 79 (2012).

[205] *See* NAT'L ASS'N OF CORP. DIR., 2019-2020 NACD PUBLIC COMPANY GOVERNANCE SURVEY 20 (2019).

[206] Trautman et al., *supra* note 196, at 511.

> So, one of the things that I view as our keen responsibility is to listen, understand, and make sure that there's mitigation and other attention being given alongside with outside benchmarking. But to me, one of my primary responsibilities is to make sure that the cyber teams have enough resources to do the job in today's world. Part of the problem is that in many organizations the budget within the cyber and the information area has been increasing enormously. And part of our responsibility on the audit committee and full board is protecting the employees that are in cyber functions and ensuring that management provides the attention and the resources that are needed.
>
> It is important that boards explore bringing an individual with cyber experience on to the board. However, in the absence of such cyber talent, one of the ways in which we manage is to have outside experts that come into the boardroom and talk to us. And one of the reasons that we tend to do it that way is that we found that cyber developments and the risks around cyber change so much. We found that if we brought somebody who's retired, that their knowledge goes stale very quickly. And so that's how we tend to handle it. The other pandemic development is that the business environment is going virtual. As a result, ransomware is an area that is exploding in terms of risk—and boards need to be aware and focused on ransomware.[207]

Director Ron McCray states, "In my experience, I have seen cyber risk handled a couple of different ways."[208] He continues:

---

[207] *See id.* at 511–12 (citing Lawrence J. Trautman et al., *Posted: No Phishing*, 8 EMORY CORP. GOV. & ACCT. REV. 39 (2021) (discussing ransomware threats)); *see also* Hon. Bernice Donald et al., *Crisis at the Audit Committee: Challenges of a Post-Pandemic World*, REV. BANKING & FIN. L. (forthcoming) (ms. at 33), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4240080; Lawrence J. Trautman et al., *Governance of The Internet of Things (IoT)*, 60 JURIMETRICS 315, 327 (2020) (discussing ransomware common threat vectors).

[208] *See* Trautman et al., *supra* note 196, at 511.

> I serve on the board and on the audit committee of a major research university. And if you think about the kind of exposure that university would have . . . [w]e have a subcommittee of the audit committee that's focused on cyber security and it's populated with trustees who have functional executive experience in the cyberspace. Contrasted with another company board on which I serve . . . [i]n this situation, we don't have a cyber security expert. Without board cyber security expertise, what we do have is a regular dialogue with the chief technology officer. And so we manage the risk by giving keen oversight over what that CTO is seeing . . . and to the extent he or she can identify risk—we monitor what they're doing about managing, mitigating, or eliminating it.[209]

E. *Lessons from Recent Experience*

Professor Chang recently observes, "During this pandemic, cyber intrusions have increased dramatically. Just because everybody's online so much, including the shift toward employees working from home. A board has to decide whether there is enough cyber talent on the board, just to understand the complexity of issues."[210] Professor Chang further states:

> Another issue worth mentioning here relates to the legal consequences of cyber and data privacy issues. Depending on the company's domicile and where business is being conducted—if in Texas, or if it's in California, or it's in New York—jurisdictions have different laws about disclosure. So, if you get breached, it turns out there are numerous different disclosure laws that a company must comply with. And legislation is constantly changing these requirements. It's really important that directors understand the legal consequences of a cyber breach in their company, in their state, in their industry. Conse-

---

209 *Id.*

210 *Id.* at 510.

> quences are different in the healthcare industry, different in retail, different in finance, and it's different in education. So it's really important that directors understand the legal environment in which they are operating.[211]

Director Ron McCray states, "In my last CEO job, I elevated the chief technology officer (CTO) to my leadership team."[212] He continues:

> We wanted all of the operating executives to have visibility into what the data function team was seeing around the company—and therefore, to have detailed insight into what all the operators were living. When we had board meetings, all of my leadership team joins me in board meetings. Therefore, we have a natural opportunity to elevate cyber security issues in the audit committee and among the full board. In addition, this format allows for the directors, the CTO and I as CEO, to all engage productively on the topic and to better identify the risks.[213]

Director Ron McCray observes, "Most companies probably have some sort of redundancy defense deployed, so that if they are hit by something from cyberspace, data systems are backed-up and easily recoverable. Every enterprise must have the ability to get up and running from somewhere else."[214] Fred Chang adds, "There are plenty of examples of corporations that have moved some data operations from one part of the country to another part of the country for both cost and redundancy reasons." Professor Chang warns:

---

[211] *Id.*; *see also* David D. Schein & Lawrence J. Trautman, *The Dark Web and Employer Liability*, 18 COLO. TECH. L.J. 49, 76 (2020); Lawrence J. Trautman et al., *Some Key Things U.S. Entrepreneurs Need to Know About the Law and Lawyers*, 46 TEX. J. BUS. L. 155, 165 (2016); Lawrence J. Trautman et al., *Teaching Ethics and Values in an Age of Rapid Technological Change*, 17 RUTGERS BUS. L. REV. 17, 37 (2021) (discussing ethical and legal issues).

[212] Trautman et al., *supra* note 196, at 512.

[213] *See id.* at 510.

[214] *Id.* at 514.

> Cyber is one of these asymmetric attacks where directors can provide corporate cyber defenders with a big check, but, for a relatively small amount of money, an attacker can successfully get through defenses. So, while the defender has to defend a bunch of different positions, all the attacker has to do is find a way through one position . . . one port or one human clicking on a link that they shouldn't. Therefore, these situations are very difficult because an attacker doesn't have to spend too much in resources to do considerable damage, while the defender has spent a lot of money to create a fortress that is unfortunately, ultimately compromised. This is why these attacks are referred to as asymmetric.[215]

Cyber expert Frederick R. Chang further states, "Michelle Hooper brings up a good point about budgets."[216] Consider:

> I talk with plenty of chief information security officers (CISOs) where they say, "the board has given me lots of money to protect against a cyber breach. But, I don't have the people to spend all the money or I don't have all the talent to spend all the money so . . . I can't protect everything, even if you gave me five times the budget. I just, can't do it . . . don't have the time. There aren't enough hours in the day."
>
> There should be an expectation that board members have of management—about having an analytical framework (dashboard) in which to measure risk. So, companies should ascribe a measurable risk of a weather event, a power loss event, a cyber event, or other event—and provide contingency plans for each. A gameplan must exist ahead of time to decide steps to be taken in the event of a cyber breach, weather risk, a power outage, etc. This discipline provides a framework to help decide what resources are dedicated toward the different risks. This allows

---

215 *Id.*

216 *Id.* at 512.

> management to have a framework to analyze these threats.[217]

F. *A Formal Plan for Cyber Crisis*

Seasoned directors recognize and best practices dictate that "a clear strategy and implementation plan for reasonably foreseeable industry disasters—before they take place, helps to prevent mistakes made under conditions of severe stress."[218] By now, cyber breach has become a reasonably foreseeable event. As such, having written procedures and practicing mock breaches seems a reasonable management procedure. Director Ron McCray states, "I found it useful in every company where I've served to have a crisis management manual."[219] Consider:

> This manual delineates principal risks that might attend to the enterprise. And it gives management a rough outline or map of how they should think about managing those risks. And every once in awhile, like you would with a fire risk, you have a fire-like drill to test drive the crisis management manual. This is one way that I have found effective to assure that through regular crisis 'fire drills' acquaintance with the risk management framework that we develop for crisis management is reinforced.[220]

---

[217] *Id.* at 512–13; *see also* Fred Chang, *Sputnik Offers a Lesson on Cybersecurity Workforce*, DALL. MORNING NEWS (Oct. 3, 2017, 12:25 PM), https://www.dallasnews.com/opinion/commentary/2017/10/03/sputnik-offers-a-lesson-on-cybersecurity-workforce (discussing cyber workforce shortage); Mohammed Hussein et al., *Technology Employment, Information and Communication in the Digital Age*, 103 J. PAT. & TRADEMARK OFF. SOC'Y 101, 103 (2023) (discussing information technology/cybersecurity employment opportunities).

[218] Lawrence J. Trautman, *The Board's Responsibility for Crisis Governance*, 13 HASTINGS BUS. L.J. 275, 275 (2017); *see also* Marianne M. Jennings & Lawrence J. Trautman, *Ethical Culture and Legal Liability: The GM Switch Crisis and Lessons in Governance*, 22 B.U. J. SCI. & TECH. L. 187, 187–88 (2016).

[219] Trautman et al., *supra* note 196, at 515.

[220] *Id.*

G. *SEC Actions Regarding Data Breaches*

Recent cases show that the SEC's Division of Enforcement is focusing on cybersecurity, including a focus on advisers' compliance with adopted policies and procedures.[221] Much of the recent focus has been on companies not maintaining proper procedures and safeguards for preventing data breaches.[222] Additionally, recent cases also focus on how companies react to prevent breaches, including timely remediation of those breaches and how information about a breach is timely and publicly disclosed.[223]

H. *The Safeguards Rule*

To protect against disclosure of private consumer information, the Gramm-Leach-Bliley Act ordered various government agencies to establish rules to protect consumer information maintained by financial institutions.[224] These rules became known as "Safeguards Rules."[225] In 2005, the SEC adopted its Safeguards Rules in 17 C.F.R. § 248.30(a), as part of Regulation S-P.[226] The SEC's Safeguards Rules state:

> (a) Every broker, dealer, and investment company, and every investment adviser registered with the Commission must adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. These written policies and procedures must be reasonably designed to:
>
> > (1) Insure the security and confidentiality of customer records and information;

---

[221] Michael Osnato et al., *Key Takeaways from Recent SEC Cybersecurity Charges*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Oct. 1, 2011), https://corpgov.law.harvard.edu/2021/10/01/key-takeaways-from-recent-sec-cybersecurity-charges.

[222] *Id.*

[223] *Id.*

[224] 15 U.S.C. § 6801.

[225] Dean William Harvey & Amy White, *The Impact of Computer Security Regulation on American Companies*, 8 TEX. WESLEYAN L. REV. 505, 522 (2002).

[226] Privacy of Consumer Financial Information (Regulation S-P), 17 C.F.R. § 248.30(a) (2005).

> (2) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
>
> (3) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.[227]

In 2021, the SEC sanctioned eight companies in three actions under its Safeguards Rule for failures in their cybersecurity policies and procedures which led to takeovers of the companies' email accounts, which exposed personal information of the clients of the firms.[228]

Cetera alleged that the Cetera Entities[229] failed to adopt policies and procedures designed to protect customer records and information.[230] The Cetera Entities were registered broker-dealers and investment advisors which offered a wide range of investment products and services through a network of independent contractors.[231] Between 2017 and 2020, the Cetera Entities used cloud-based email services for internal and external communications.[232] These email communications often stored the Cetera Entities' customers' personally identifiable information (PII).[233] In late 2017, unauthorized third parties used phishing, credential stuffing, and other modes of attack to take over thirty-two of the Cetera Entities' email accounts.[234] In January 2018, the Cetera Entities turned on multi-factor authorization (MFA) to ensure that users would need to log on using

---

227 *Id.*

228 Press Release, Sec. & Exch. Comm'n, SEC Announces Three Actions Charging Deficient Cybersecurity Procedures (Aug. 30, 2021), https://www.sec.gov/news/press-release/2021-169.

229 Cetera Advisor Networks LLC, Exchange Act Release No. 92800, 2021 WL 3860254, at *1 (Aug. 30, 2021). *Cetera* was a consolidated action brought against Cetera Advisor Networks LLC, Cetera Investment Services LLC, Cetera Investment Services LLC, Cetera Financial Specialists LLC, and Cetera Investment Advisers LLC (hereinafter the "Cetera Entities"). *Id.*

230 *Id.*

231 *Id.* at *3.

232 *Id.*

233 *Id.*

234 *Id.* at *4.

MFA.[235] In February 2018, the Cetera Entities' policies required MFA to be turned on "wherever possible."[236] In September 2018, approximately 1,500 contractors' email accounts were identified that did not have MFA turned on.[237] The policies were amended in October 2018 to require the use of MFA "wherever possible, but at a minimum for privileged or high-risk access."[238] During 2018 and 2020, approximately thirty more of the Cetera Entities' representatives' email accounts were taken over, resulting in the exposure of over 2,700 customers' PII.[239] Despite the Cetera Entities' MFA policy, none of the email accounts that were taken over had MFA turned on.[240] Additionally, the Cetera Entities did not include MFA for their offshore contractors' email accounts until the end of 2019.[241] This resulted in four offshore contractors' accounts being taken over and the exposure of 1,662 more customers' PII.[242]

After each account takeover, the Cetera Entities identified which customers had their PII exposed, and those customers were issued breach notifications.[243] The breach notifications were prepared by outside counsel.[244] Approximately 220 of the letters that were sent included misleading "template language" regarding the timing of the breaches.[245] The brief notifications stated that the email accounts were recently breached and that unauthorized access to the customers' PII was two months before the notifications being sent.[246] The dates of the notifications reflected when the attorneys' review was complete, not when Cetera Entities had learned of the breaches, which was six months prior.[247] The Cetera Entities had a policy in place that required their own personnel review client communications regarding cybersecurity incidents before the communications

---

235 *Cetera*, 2021 WL 3860254, at *4.
236 *Id.* at *3.
237 *Id.* at *4.
238 *Id.* at *3.
239 *Id.* at *4.
240 *Id.*
241 *Cetera*, 2021 WL 3860254, at *4.
242 *Id.*
243 *Id.*
244 *Id.*
245 *Id.*
246 *Id.*
247 *Cetera*, 2021 WL 3860254, at *4.

were sent.[248] Because there was no adequate internal review correcting the template language, the SEC found that the brief notifications were "misleading in light of the circumstances known to the firms at the time of the review."[249] The SEC charged that the policy violation was a willful violation of the Safeguards Rule for not adopting "written policies and procedures that are reasonably designed to safeguard customer records and information."[250] The SEC ordered the Cetera Entities to pay a $300,000 civil penalty.[251]

Cambridge also involved a violation of the Safeguards Rule by Cambridge Investment Research and Cambridge Investment Research Advisors (together, Cambridge).[252] Cambridge has approximately 4,750 registered representatives, with approximately 4,330 whom are registered with FINRA as independent contractors.[253] An information security group at Cambridge's headquarters provided its independent representatives with cybersecurity guidance and policies and procedures.[254] However, each independent representative was individually responsible for implementing these cybersecurity policies and procedures.[255] Cambridge recommended that its independent representatives implement MFA and other enhanced security measures on the email systems, but none of the security measures were mandated.[256] Between January 2018 and July 2021, Cambridge discovered that 121 independent representatives' email accounts were taken over by unauthorized third parties on its cloud-based email system.[257] Cambridge's brokerage customers' PII was emailed and stored on this email system.[258] The compromised ac-

---

248 *Id.* at *5.
249 *Id.*
250 *Id.*
251 *Id.*
252 Cambridge Inv. Rsch., Inc., Exchange Act Release No. 92806, 2021 WL 3860259, at *1–2 (Aug. 30, 2021).
253 *Id.* at *2.
254 *Id.*
255 *Id.*
256 *Id.*
257 *Id.* at *3.
258 *Cambridge*, 2021 WL 3860259, at *2.

counts led to 2,177 customers' PII being exposed and intruders forwarding the PII to an external third-party account.[259] Cambridge notified these customers of the breach and offered the impacted customers identity theft protection services.[260] Additionally, Cambridge notified an additional 3,800 customers that they had been subjected to phishing attacks.[261] The email takeovers did not lead to any of Cambridge's customer accounts being subject to unauthorized trades or fund transfers.[262]

After discovering the email takeovers, Cambridge suspended the affected independent contractors' email accounts and reset their passwords.[263] Until July 2021, Cambridge continued its policy of recommending, but not requiring, that these independent contractors enhance their email security by using MFA.[264] Although some of the independent representatives followed Cambridge's recommendation, many did not.[265] In July 2021, Cambridge amended its policy and required MFA to be used on independent representatives' cloud-based email accounts.[266] The SEC found that Cambridge violated the Safeguards Rule by not adopting written policies and procedures that were reasonably designed to safeguard customer records and information.[267] Cambridge was censured and ordered to pay a civil money penalty of $250,000.[268]

The SEC also alleged a violation of the Safeguards Rule in *KMS Financial Services*.[269] KMS Financial Services (KMS) was registered as a broker-dealer and an investment advisory firm.[270] Between September 2018 and August 2020, KMS offered services through a network of 400 independent contractors acting as financial advisers.[271] KMS had policies in place that required its advisers to

---

259 *Id.* at *3.
260 *Id.*
261 *Id.*
262 *Id.*
263 *Id.*
264 *Cambridge*, 2021 WL 3860259, at *3.
265 *Id.*
266 *Id.*
267 *Id.* at *4.
268 *Id.*
269 KMS Fin. Servs., Inc., Exchange Act Release No. 92807, 2021 WL 3860263 at *1 (Aug. 30, 2021).
270 *Id.* at *2.
271 *Id.*

"[c]onduct [their] business practices in a way that safeguards the confidentiality of [their] client's identity, including protecting all sensitive client information" and to "[p]eriodically review [their] internal business policies to make sure they are adequately designed to protect sensitive client information."[272] Further policy called for the use of strong passwords, securing wireless networks, using antivirus and malware protection, securing backup and stored data, and encrypting hard drives.[273] Fifteen KMS financial advisers suffered account takeovers that resulted in exposure of 4,900 customers' PII.[274] After the breach, it took twenty-one months for security measures to be adopted firm-wide.[275] These measures included resetting the affected financial advisers' email passwords, removing forwarding rules, and enabling MFA.[276] Also, KMS did not have its own Incidence Response Policy and instead used one adopted by another subsidiary of its parent company, which did not include guidelines on timeframes or schedules for response activities.[277] The elongated timeline for the implementation of the safety measures and the lack of timeline for response activities left the security of additional customer records and information at risk.[278] KMS's lack of adopting written policy and procedures designed to safeguard customer records and information led to the SEC finding that KMS violated the Safeguards Rule.[279] KMS was censured and ordered to pay a civil money penalty of $200,000.[280]

I. *Failure to Timely Remediate a Breach*

The SEC has not limited its concerns with cybersecurity breaches to violations of the Safeguards Rule. *Cetera*, *Cambridge*, and *KMS* followed shortly after two other actions in which the SEC addressed cybersecurity breaches. In June 2021, the SEC brought

---

272 *Id.*
273 *Id.*
274 *Id.* at *3.
275 *KMS Fin. Servs.*, 2021 WL 3860263, at *3.
276 *Id.*
277 *Id.*
278 *Id.*
279 *Id.* at *4.
280 *Id.*

First American Financial Corp.[281] In May 2019, First American Financial Corporation (First American) was notified by a cybersecurity journalist that one of its applications had a vulnerability which exposed over 800 million title and escrow document images, which included personal data such as social security numbers and financial information.[282] The application, EaglePro, was used to transmit title and escrow related documents to First American customers.[283] First American, after being alerted of the breaches by the journalist, provided the following statement for inclusion in an article on the breaches:

> First American has learned of a design defect in an application that made possible unauthorized access to customer data. At First American, security, privacy and confidentiality are of the highest priority and we are committed to protecting our customers' information. The company took immediate action to address the situation and shut down external access to the application.[284]

Later that same week, First American filed a Form 8-K which attached a press release stating that there was "[n]o preliminary indication of large-scale unauthorized access to customer information"[285] and also that "First American Financial Corporation advises that it shut down external access to a production environment with a reported design defect that created the potential for unauthorized access to customer data."[286] However, First American security personnel had done a test prior to the journalist's story and created a report in January 2019 indicating that there were security vulnerabilities in the EaglePro application.[287] Some of First American's senior technical experts were aware of the report, including the

---

[281] First Am. Fin. Corp., Exchange Act Release No. 92176, 2021 WL 2439179, at *1 (June 14, 2021).

[282] *Id.*

[283] *Id.* at *2.

[284] *Id.* at *4.

[285] *Id.*

[286] *Id.* at *4.

[287] *First Am. Fin. Corp.*, 2021 WL 2439179, at *3.

CISO and CIO, prior to the issuance of the 8-K.[288] However, the report was not made available to First American's senior executives—including the CEO and CFO—prior to making the press statements or issuing the 8-K.[289] The SEC charged that First American violated Exchange Act Rule 13a-15(a), which "requires registered companies to maintain disclosure controls and procedures that are designed to ensure that information required to be disclosed by the issuer in the reports that it files or submits under the Act . . . is recorded, processed, summarized and reported, within the time periods specified" by the SEC.[290] Because the information in the security team's report was not furnished to First American's senior management, the information could not be properly evaluated when they approved the press releases and the issuance of the 8-K.[291] First American was ordered to pay a civil penalty of $487,616.[292]

J. *Failure to Properly Make Proper Public Disclosures About a Breach*

The SEC also brought *Pearson* in 2021, which was concerned with knowledge of a breach not being publicly disseminated.[293] Pearson is an educational publishing company that delivers academic performance assessments to school districts.[294] In March 2019, Pearson learned that millions of rows of data stored on its AIMSweb 1.0 server had been accessed and downloaded by a sophisticated threat actor.[295] The data that was compromised included all school district personnel usernames and passwords, as well as student data that included student names, birthdays, and email addresses.[296] The software's vulnerability was publicized by the manufacturer and a patch was offered to Pearson in September 2018.[297] Pearson did not implement the patch until after it found out about

---

288 *Id.* at *5.
289 *Id.*
290 17 C.F.R. § 240.13a-15 (a), (e) (2023).
291 *First Am. Fin. Corp.*, 2021 WL 2439179, at *5.
292 *Id.* at *6.
293 Pearson PLC, Exchange Act Release No. 10963, 2021 WL 3627064, at *1 (Aug. 16, 2021).
294 *Id.* at *2.
295 *Id.*
296 *Id.*
297 *Id.*

the data breach.[298] Pearson created an incident management response team to investigate the breach, but decided not to issue a public statement about the incident at that time.[299] In July 2019, Pearson issued a Form 6-K for January through June 2019.[300] In the 6-K, Pearson listed as "[p]rincipal risk and uncertainties" that there was:

> [Risk] of a data privacy incident or other failure to comply with data privacy regulations and standards and/or a weakness in information security, including a failure to prevent or detect a malicious attack on our systems, could result in a major data privacy or confidentiality breach causing damage to the customer experience and our reputational damage, a breach of regulations and financial loss.[301]

Pearson's language in the Form 6-K was the same as was used in previous 6-K reports, so it implied that no major breach had occurred, although Pearson had known about the breach for months.[302]

On July 31, 2019, after being contacted by a reporter about the data breach, Pearson then released a media statement about the breach.[303] The SEC found the statement was misleading because it did not mention that data was removed from the server, it did not properly describe all of the data that was breached and how much of that data was exfiltrated, and some statements about which data was compromised was described as hypothetically breached even though the data was known to have been breached.[304] The day after issuing the media statement, Pearson's price declined by 3.3%.[305] Based on the misleading disclosures, the SEC charged Pearson with offering and selling securities by untrue statements of material fact or omission which would make a statement not misleading, in violation of Sections 17(a)(2) and 17(a)(3) of the Securities Act.[306] Pearson was

---

298 *Id.*
299 *Pearson*, 2021 WL 3627064, at *2.
300 *Id.* at *3.
301 *Id.*
302 *Id.*
303 *Id.*
304 *Id.*
305 *Pearson*, 2021 WL 3627064, at *4.
306 *Id.*

also charged with violating the Securities Exchange Act Section 13(a) by filing inaccurate periodic reports and Rule 13a-15 failing to maintain proper disclosure controls and procedures.[307] Pearson was offered to pay a civil money penalty in the amount of $1,000,000.[308]

K. *2023 SEC Cybersecurity Rule Adoption*

For many years, there were calls for the SEC to adopt specific rules requiring disclosure of cybersecurity breaches as those could affect the value of the company's publicly traded securities.[309] On July 26, 2023, the SEC adopted rules that require registrants "to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance."[310] This announcement was long anticipated because the European Union had adopted the General Data Protection Regulation (GDPR) in 2018.[311] The GDPR is a broad privacy act that allows a consumer to have their data deleted from company databases, requires companies to notify consumers if their information is breached, and has penalties for failure to do so.[312] Ironically, while being a key cybersecurity protection, the penalty provisions seem to be a new vehicle of extortion in ransomware campaigns. RansomedVC, the hacker group

---

307 *Id.* at *5.

308 *Id.*

309 *See, e.g.*, Porath, *supra* note 100, at 145; Norah C. Avellan, *The Securities and Exchange Commission and the Growing Need for Cybersecurity in Modern Corporate America*, 54 WASHBURN L.J. 193, 225 (2014); Michael Hooker & Jason Pill, *You've Been Hacked, and Now You're Being Sued: The Developing World of Cybersecurity Litigation*, 90 FLA. B.J., 30, 39 (July/Aug. 2016); Neal F. Newman & Lawrence J. Trautman, *Securities Law: Overview and Contemporary Issues*, 16 OH. ST. BUS. L.J. 149 (2021), http://ssrn.com/abstract=3790804; Neal F. Newman & Lawrence J. Trautman, *A Proposed SEC Cyber Data Disclosure Advisory Commission,* 50 SEC. REG. L.J. 199 (2022), http://ssrn.com/abstract=4097138; Lawrence J. Trautman & George P. Michaely, *The SEC & The Internet: Regulating the Web of Deceit*, 68 CONSUMER FIN. L.Q. REP. 262 (2014), http://www.ssrn.com/abstract=1951148.

310 Press Release, Sec. & Exch. Comm'n, SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (July 26, 2023) https://www.sec.gov/news/press-release/2023-139.

311 Siegel, *supra* note 38, at 214.

312 *Id.* at 194.

that alleged that it breached Sony's systems, based some threats on proof of companies violating the GDPR rules, which could lead to fines greater than the amount of the ransoms demanded.[313] However, GDPR is largely credited with causing cybersecurity breaches to be discovered faster, lessening the amount of time hackers spend in compromised organizations.[314] One major provision of the GDPR is that it applies to foreign companies when doing business in the EU, so major U.S. companies have been subjected to it since its outset.[315] California took the lead in cybersecurity legislation in the U.S.; in 2020, California enacted the California Consumer Privacy Act (CCPA), borrowing many concepts on consumer privacy and reporting from the GDPR.[316] The CCPA made the California Private Protection agency "the first government body in the United States with the sole job of regulating how Google, Facebook, Amazon and other companies collect and use data from millions of people."[317]

The SEC press release on Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure announced new rules relating to cybersecurity, which apply to both domestic and foreign issuers.[318] The new rules require that a registered company file a Form 8-K within four days of a cybersecurity incident they determine to be material and to describe the material aspects of the incident's nature, scope, and timing, as well as its material impact or reasonably likely material impact on the registrant.[319] There is a national security exception that allows for the disclosure to be delayed "if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public

---

313 Williams, *supra* note 6.

314 Danny Palmer, *Cybersecurity: Hacking Victims are Uncovering Cyberattacks Faster - and GDPR Is the Reason Why*, ZDNET (Feb. 20, 2020), https://www.zdnet.com/article/cybersecurity-hacking-victims-are-uncovering-cyber-attacks-faster-and-gdpr-is-the-reason-why.

315 Siegel, *supra* note 38, at 214–15.

316 California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.1 (2018).

317 David McCabe, *How California Is Building the Nation's First Privacy Police*, N.Y. TIMES (Mar. 15, 2022), https://www.nytimes.com/2022/03/15/technology/california-privacy-agency-ccpa-gdpr.html.

318 Press Release, Sec. & Exch. Comm'n, *supra* note 310.

319 *Id.*

safety and notifies the Commission of such determination in writing."[320] The SEC rule also requires registrants to disclose any processes it has "for assessing, identifying, and managing material risks from cybersecurity threats, as well as the material effects or reasonably likely material effects of risks from cybersecurity threats and previous cybersecurity incidents."[321] Registrants will also be required to include a statement in their 10-K describing its board's oversight of cybersecurity risks and the board's expertise in assessing and managing those risks.[322]

On September 21, 2023, the *Wall Street Journal* reported, "A cyberattack on cleaning-products maker Clorox is providing an early test for new rules on disclosing cyberattacks, in a case that is being closely watched by business leaders."[323] Clorox was one of the first major U.S. companies to be victimized by a cyberattack since the SEC issued its new cybersecurity rules.[324] On August 14, 2023, Clorox issued a Form 8-K stating that it had "identified unauthorized activity on some of its Information Technology (IT) systems."[325] Clorox further noted that they were taking remedial steps including taking some of its systems offline.[326] After this initial Form 8-K, Clorox issued further 8-K filings adding details about its disruptions to operations.[327] On September 18, 2023, Clorox noted in another Form 8-K that it had contained the unauthorized activity within its systems.[328] Clorox further noted that the extent of the damage to its infrastructure and the financial implications were still unknown, and it did not know how long it would take to restore normal operations.[329] It was noted that "Clorox's string of bulletins over more than four weeks shows how determining the material impact

---

320 *Id.*

321 *Id.*

322 *Id.*

323 Kim Nash, *Clorox Cyberattack Tests New Rules on Disclosure*, WALL ST. J. (Sept. 20, 2023, 5:30 AM), https://www.wsj.com/articles/clorox-cyberattack-brings-early-test-of-new-sec-cyber-rules-b320475.

324 *Id.*

325 The Clorox Co., Current Report (Form 8-K), at Item 8.01 (Aug. 14, 2023).

326 *Id.*

327 Nash, *supra* note 323.

328 The Clorox Co., Current Report (Form 8-K), at Item 8.01 (Sept. 18, 2023).

329 *Id.*

of a cyberattack is unfamiliar ground for companies."[330] However, the new SEC rules did seem to ensure that there was timely and thorough reporting of the situation to the investing public.

V. EMERGING THREAT OF NATION-STATES AND GEOPOLITICS

In many ways, 2021 marked a watershed moment for cybersecurity as it became a front-burner issue in major geopolitical discussions including the G7 and during a major bilateral Geneva summit between Presidents Biden and Putin.[331] Among other developments, both the UN's Open-Ended Working Group (OEWG) and Group of Governmental Experts (GGE) released a consensus report that, among other developments, reinforced support by the international community for eleven cyber norms, which may be considered rules of the road guiding state behavior in cyberspace.[332] It is notable that the United States, China, and Russia have all agreed to this list of norms, as encapsulated in Exhibit 10.

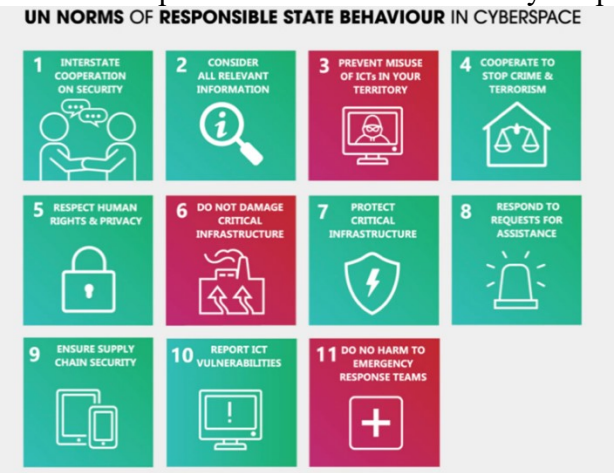
---

330 Nash, *supra* note 323.

331 *See* Jonathan Grieg, *Biden and Putin Spar Over Cybersecurity, Ransomware at Geneva Summit*, ZDNET (June 16, 2021, 6:50 PM), https://www.zdnet.com/article/biden-and-putin-spar-over-cybersecurity-ransomware-at-geneva-summit.

332 Josh Gold, *Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?*, COUNCIL ON FOREIGN REL. (Mar. 18, 2021, 11:41 AM), https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what.

EXHIBIT 10
UN Norms of Responsible State Behavior in Cyberspace[333]



Further, the United States made headlines for finally joining the Paris Call for Trust and Security in Cyberspace, which is "a multi-stakeholder statement of principles designed to help guide the international community toward greater cyber stability."[334] On the day it was announced, more than fifty nations, along with "130 companies and 90 universities and nongovernmental groups" signed the Paris Call, a coalition that grew to eighty nations and over 600 companies by early 2022.[335] The United States was a notable holdout, given

---

[333] *Eleven Norms of Responsible State Behaviour in Cyberspace*, FDFA (July 4, 2021), https://www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2021/04/uno-cyber-normen.html.

[334] Scott J. Shackelford et al., *Rethinking Active Defense: A Comparative Analysis of Proactive Cybersecurity Policymaking*, 41 U. PA. J. INT'L L. 377 (2020).

[335] David E. Sanger, *U.S. Declines to Sign Declaration Discouraging Use of Cyberattacks*, N.Y. TIMES (Nov. 12, 2018), https://www.nytimes.com/2018/11/12/us/politics/us-cyberattacks-declaration.html; *Indiana University Among First to Endorse Paris Call for Trust and Security in Cyberspace*, NEWS AT IU (Nov. 12, 2018), https://news.iu.edu/stories/2018/11/iu/releases/12-paris-call-for-trust-and-security-in-cyberspace.html; *Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*, FRANCE DIPLOMATIE, https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in (last updated Feb. 2021).

that the rest of the Five Eyes nations had already joined the initiative, which provides another forum for the United States and its allies to pressure state sponsors of ransomware groups.[336]

Looking ahead, the geopolitics of cybersecurity remain treacherous, but because these eleven cyber norms are now widely recognized, multilateral and multi-stakeholder discussions will pivot to operationalizing and enforcing them.[337] This includes the need to clarify cybersecurity due diligence and governance best practices in partnership with the private sector.

A. *How Business Works with Government on Cybersecurity*

Cybersecurity is, in essence, a public-private partnership requiring active and sustained participation from engaged stakeholders. Too often, for example, public-private partnerships become a one-way street in which private firms share their cyber threat data with the government, but often get little back in return. The same can be said for state officials, who often complain of a lack of robust information sharing on the part of their federal counterparts.[338] This may be seen in particular in the context of election security.[339] The growth of broad-based Information Sharing and Analysis Organizations (ISAOs) championed by the Obama Administration may be seen as a step in this direction.[340] However, a great deal of work has also been done pointing in the opposite direction, e.g., that rather than broadening the pool of information sharing partners, the most effective sharing in fact takes place among trusted groups of relative

---

[336] *See* Sean Lyngaas, *US Joins International Cybersecurity Partnership that Trump Snubbed*, CNN (Nov. 10, 2021, 5:39 PM), https://www.cnn.com/2021/11/10/politics/us-paris-cybersecurity-agreement/index.html.

[337] For a discussion of how this is playing out in the context of cybersecurity due diligence, see Scott J. Shackelford et al., *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. INT'L L. 1 (2016).

[338] GAO, CRITICAL INFRASTRUCTURE PROTECTION: NATIONAL CYBERSECURITY STRATEGY NEEDS TO ADDRESS INFORMATION SHARING PERFORMANCE MEASURE AND METHODS (2023).

[339] GAO, ELECTION SECURITY, DHS PLANS ARE URGENTLY NEEDED TO ADDRESS IDENTIFIED CHALLENGES BEFORE THE 2020 ELECTION (2020), https://www.gao.gov/products/gao-20-267.

[340] *See* Exec. Order No. 13,636, *supra* note 115; Exec. Order No. 13,691, *supra* note 127.

insiders.[341] At the least, state and federal officials should entice more robust information sharing by promising a return on investment, such as real-time threat analysis of the type now being pioneered by the FBI.

To help guard against the most sophisticated cyberattackers, which can include nation-states, it is also important for government to work alongside the private sector in matters of attribution. This may be seen as part of the larger movement on proactive cybersecurity in which firms use active defense best practices such as machine learning, deep packet inspection, cybersecurity analytics, and even cyber risk insurance to mitigate their cyber risk by making deterrence more effective. Ultimately, though, to deter nation-states, it becomes vital to raise the overall level of cybersecurity due diligence across the U.S. economy, which is far easier said than done. However, the National Institute for Standards and Technology (NIST) Cybersecurity Framework may be seen as a positive step forward in this regard.

Government can also be a positive force in encouraging firms to treat cybersecurity as a shared, social responsibility, an ideal to which DHS has previously alluded. Such an approach moves firms beyond stale debates about importing the tools of cost-benefit analysis and the like to cybersecurity decision-making, and instead encourages stakeholders across the Internet ecosystem to bolster their defenses.

VI. IDENTIFYING AND RESPONDING TO DIGITAL ATTACKS

A. *What U.S. Companies Can Do About Cyber Threat*

Among those tangible steps that all enterprises can take to advance cyber resilience is to become familiar with the many resources

---

[341] WORLD ECON. F., CYBER INFORMATION SHARING: BUILDING COLLECTIVE SECURITY 4 (2020), https://www3.weforum.org/docs/WEF_Cyber_Information_Sharing_2020.pdf.

that have now become available, including CISA,[342] NIST,[343] and the SEC,[344] just to name a few.

In a January 2017 publication titled *Advancing Cyber Resilience: Principles and Tools for Boards*, the World Economic Forum provides the following Board Principles for Cyber Resilience, provided at Exhibit 11.[345]

EXHIBIT 11
Board Principles for Cyber Resilience[346]

Principle 1

Responsibility for cyber resilience. The board as a whole takes ultimate responsibility for oversight of cyber risk and resilience. The board may delegate primary oversight activity to an existing committee (e.g. risk committee) or new committee (e.g. cyber resilience committee).

Principle 2

Command of the subject. Board members receive cyber resilience orientation upon joining the board and are regularly updated on recent threats and trends – with advice and assistance from independent external experts being available as requested.

Principle 3

Accountable officer. The board ensures that one corporate officer is accountable for reporting on the organization's capability to manage cyber resilience and progress in implementing cyber resilience goals. The board ensures that this officer has regular board access, sufficient authority, command of the subject matter, experience and resources to fulfil these duties.

Principle 4

Integration of cyber resilience. The board ensures that management integrates cyber resilience and cyber risk assessment into overall business strategy and into enterprise-wide risk management, as well as budgeting and resource allocation.

Principle 5

Risk appetite. The board annually defines and quantifies business risk tolerance relative to cyber resilience and ensures that this is consistent with corporate strategy and risk appetite. The board is advised on both current and future risk exposure as well as regulatory requirements and industry/societal benchmarks for risk appetite.

Principle 6

Risk assessment and reporting. The board holds management accountable for reporting a quantified and understandable assessment of cyber risks, threats and events as a standing agenda item during board meetings. It validates these assessments with its own strategic risk assessment using the Board Cyber Risk Framework.

Principle 7

Resilience plans. The board ensures that management supports the officer accountable for cyber resilience by the creation, implementation, testing and ongoing improvement of cyber resilience plans, which are appropriately harmonized across the business. It requires the officer in charge to monitor performance and to regularly report to the board.

Principle 8

Community. The board encourages management to collaborate with other stakeholders, as relevant and appropriate, in order to ensure systemic cyber resilience.

Principle 9

Review. The board ensures that a formal, independent cyber resilience review of the organization is carried out annually.

Principle 10

Effectiveness. The board periodically reviews its own performance in the implementation of these principles or seeks independent advice for continuous improvement.

---

342 *See Cybersecurity Alerts and Advisories*, CISA, https://www.cisa.gov/news-events/cybersecurity-advisories (last visited Mar. 6, 2024).

343 *Cybersecurity*, NIST, https://www.nist.gov/cybersecurity (last visited Mar. 6, 2024).

344 SEC Press Release 2023-139, SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (July 26, 2023), https://www.sec.gov/news/press-release/2023-139.

345 WORLD ECONOMIC FORUM, ADVANCING CYBER RESILIENCE: PRINCIPLES AND TOOLS FOR BOARDS 8 (2017).

346 *Id.*

B. *Identifying and Responding to Digital Attacks*

Most of the attention paid to cyberattacks these days relates to truly eye-watering statistics, like Yahoo's one billion customers who had their information breached in 2016.[347] What often gets lost in the noise are the huge numbers of cyberattacks on small and medium-sized organizations that occur daily, such as the Muncie, Indiana, company Meridian Health, whose employees had their W-2s stolen after a successful phishing attack in March 2017.[348] Growing legions of cybersecurity firms have arisen to help meet the need,[349] but the variety of solutions now offered can leave managers at a loss to choose where exactly to make their next dollar of investment. This is especially true for managers and directors of small firms, some of which may be only one fraudulent wire transfer away from going out of business. Infinite investment certainly does not breed infinite security, but having a basic understanding of a core cybersecurity strategy can pay dividends, especially for small businesses. Indeed, by some estimates, 43% of cyberattackers are targeting small businesses, but only 14% rate their ability to mitigate cyber risk as "highly effective."[350] So whether it is a small law firm, a new local restaurant, or a hot tech startup, knowing the Three Bs of cybersecurity can help keep companies ahead of the cybersecurity curve: (1) be aware, (2) be organized, and (3) be proactive.[351]

---

[347] Trautman & Ormerod, *supra* note 156, at 1231.

[348] Scott Shackelford, *The Three B's of Cybersecurity for Small Businesses*, CONVERSATION (Apr. 17, 2017, 6:56 PM), https://theconversation.com/the-three-bs-of-cybersecurity-for-small-businesses-76259.

[349] *Market Research Report*, FORTUNE BUS. INSIGHTS (Apr. 2023), https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165 (reporting that the cybersecurity market is witnessing substantial growth, with forecasts suggesting a global market size increase from $172.32 billion in 2023 to $424.97 billion by 2030, and that this growth includes a wide array of cybersecurity firms offering products and services designed to protect against an expanding range of cyber threats).

[350] *Cyber Security Statistics*, PURPLESEC, https://purplesec.us/resources/cyber-security-statistics/#SmallBusiness (last visited Mar. 6, 2024).

[351] Shackelford, *supra* note 348.

C. *Be Aware*

The first step that managers and directors of small firms need to take as part of a comprehensive approach to cybersecurity risk management is to be aware of the threat environment they face—to take one concrete example, your smartphone can be turned into a microphone even when it appears powered off. In other words, you need to be informed about the different types of cyber threats and the leading tools available to help mitigate them, such as cybersecurity analytics, traffic flow analysis, and deep packet inspection. More generally, it is vital for both managers and support staff to be aware of the most common types of breaches such as phishing schemes (also known as social engineering attacks), whereby hackers try to gain access to systems by faking identities and credentials to request insiders to take actions that are against their interests, such as initiating an illegitimate wire transfer. There are a variety of tools and services available to help enhance cybersecurity awareness within organizations and help guard against cyber fatigue.[352]

D. *Be Organized*

When Sony was hacked in 2011, it did not have a Chief Information Security Officer (CISO) on staff.[353] It did by 2014, but that still did not save it from being hacked again.[354] Just like large firms, small businesses need to have a comprehensive, regularly updated, and widely disseminated incident response plan with a detailed understanding of who is responsible for what after a breach, including coordination with local law enforcement. In particular, it is vital to have frictionless coordination between employees and managers. This does not necessarily mean that your company needs to hire a CISO if it doesn't have one already, but it does mean that information security should be given equal footing with physical and personnel security. Firms that take these steps stand to save in the aftermath of a data breach.

---

352 *Cyber Security Statistics*, *supra* note 350.
353 Shackelford, *supra* note 348.
354 *Id.*

E. *Be Proactive*

At a general level, corporate cybersecurity approaches may be understood to exist along a proactivity spectrum. Many firms, especially small businesses, remain predominantly reactive—more so, perhaps surprisingly, in developed countries like the United States and the United Kingdom than businesses in emerging markets like India or China, which have been shown to be more proactive.[355] But there are a variety of tools available to help firms become more proactive. These steps include using the NIST Cybersecurity Framework to form a common vocabulary around cybersecurity risk management and to help firms identify governance gaps.[356] Some private-sector clients are already receiving the advice that if their "cybersecurity practices were ever questioned during litigation or a regulatory investigation, the 'standard' for 'due diligence' was now the NIST Cybersecurity Framework."[357] Other steps that firms can take include partnerships such as through Information Sharing and Analysis Organizations, working with universities and colleges to form cybersecurity clinics, considering the purchase of a cyber risk insurance policy, and looking to successful analogies such as the sustainability context with an array of tools such as integrated reporting and certification schemes available.

None of these suggestions are a magic bullet, but together, they can improve the unsustainable status quo and begin the process of building a culture of cyber peace. Low-hanging fruit should also not be missed, though. The Australian government, for example, has reportedly been successful in preventing 85% of cyberattacks through following three common sense techniques: application whitelisting (only permitting pre-approved programs to operate on networks), regularly patching applications and operating systems, and "minimizing the number of people on a network who have 'administrator' privileges."[358] In other words, this stuff doesn't have to be rocket science, it's just computer science.

---

[355] MCAFEE, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION 6 (2009), https://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf.

[356] *Cyber Security Statistics*, *supra* note 350.

[357] Shackelford et al., *supra* note 337, at 11.

[358] *Id.* at 18.

F. *Bounty Programs*

GitHub observes, "Software security researchers are increasingly engaging with internet companies to hunt down vulnerabilities."[359] GitHub sponsors a bounty program that advertises "rewards of up to $30,000 for more critical vulnerabilities," and publishes a bounty hunter "top ten" lists on its website.[360] Journalist Cynthia Brumfield discusses how $14 billion was stolen in cryptocurrency during 2021 alone; she writes, "The largest cryptocurrency hack so far took place last August [2021] when blockchain interoperability project Poly Network suffered a hack that resulted in a loss of over $600 million."[361] It appears that "Poly unsuccessfully attempted to publicly negotiate with the hacker a post-theft 'bug bounty' of $500,000 in exchange for returning the $600 million, a bounty worth six times more than that typically offered in traditional cryptocurrency bug bounty programs."[362]

CONCLUSION

We have shown how cyberattacks, particularly ransomware campaigns, continue to pose major threats to businesses, sovereigns, state and local governments, health and educational institutions, and individuals worldwide. Ongoing successful instances of cybercrime often involve sophisticated attacks from diverse sources such as organized-crime syndicates as seen in the rise of zero-day exploits in such operations, actors engaged in industrial espionage, nation-states, and even lone wolf actors possessing relatively few resources. Technological innovation continues to outpace the ability of law to keep pace. We believe this Article adds to the important body of cybersecurity literature that explores the roles of government and business, particularly corporate directors, in the governance of data security.

---

359 *GitHub Bug Bounty*, GITHUB SEC., https://bounty.github.com (last visited Mar. 6, 2024).

360 *Id.*

361 Cynthia Brumfield, *Skyrocketing Cryptocurrency Bug Bounties Expected to Lure Top Hacking Talent*, CSO (Feb. 17, 2022), https://www.csoonline.com/article/3649778/skyrocketing-cryptocurrency-bug-bounties-expected-to-lure-top-hacking-talent.html.

362 *Id.*