PEPPERDINE UNIVERSITY

The Journal of Business, Entrepreneurship & the Law

Volume 15 | Issue 1 Article 6

12-15-2022

Cyberattacks: An Underlying Condition Exacerbated by the COVID-19 Pandemic

Kaitlyn Palmeter

CYBERATTACKS: AN UNDERLYING CONDITION EXACERBATED BY THE COVID-19 PANDEMIC

Kaitlyn Palmeter

I. CYBERATTACKS AND THE COVID-19 PANDEMIC

In 1998, the first cyberattack, the Morris worm, "slowed down computers to the point of being unusable"[1] and damaged "10% of the entire internet."[2] By 2015, IBM CEO Ginni Rometty warned, cybercrime "is the greatest threat to … every company in the world."[3] Two years later, Cybersecurity Ventures, a leading researcher and publisher, estimated cybercrime would inflict $6 trillion in damages globally by 2021."[4] In 2020, they estimated "cybercrime damage costs could potentially double"

[1] Archana Choudhary, *The Fundamentals of Cybersecurity*, DZONE, (May 15, 2019) https://dzone.com/articles/cybersecurity-fundamentals-introduction-to-cyberse.

[2] Siobhan Climer, *History of Cyber Attacks From the Morris Worm to Exactis*, MINDSIGHT (July 3, 2018), https://gomindsight.com/insights/blog/history-of-cyber-attacks-2018/.

[3] Steve Morgan, *IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World'*, FORBES (Nov. 24, 2015, 6:46 AM), https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#705c64ac73f0.

[4] Steve Morgan, *Cybercrime To Cost The World $10.5 Trillion Annually By 2025*, CYBERCRIME MAG. (Nov. 13, 2020, 1:20 PM), https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

because of the Coronavirus pandemic.[5] COVID-19 continues to change the world in unforeseen ways triggering "a new era of corporate data breaches."[6] This article will illustrate how cyberattacks have increased in severity during the pandemic, how current laws and government officials are trying to evolve with the current threats and technology, how victims of cyberattacks risk sanctions and potential lawsuits, and concludes by suggesting solutions throughout to increase Cybersecurity.

A. *Dangerous and Prominent Cyberattack Types and Tactics*

A "cyberattack" [7] is a "deliberate exploitation of computer systems," whereby a hacker[8] executes malicious code "to alter computer code, logic or data" to cause "disruptive consequences."[9] Cyberattacks can restrict access to, remove, or alter data, and some aim to trick people into performing specific tasks.[10] Coalition, a leading cyber insurance and security firm, found that since the COVID-19 pandemic started, the most frequent types of cyberattack losses are due to ransomware (41%), fund transfers loss (27%), and business email compromise incidents (19%).[11]

---

[5] *Id.*; *see also Cybercrime damage costs may double due to Coronavirus (COVID-19) outbreak*, CISION PR NEWSWIRE (Mar. 19, 2020), https://www.prnewswire.com/news-releases/cybercrime-damage-costs-may-double-due-to-coronavirus-covid-19-outbreak-301027007.html.

[6] Tom Schmidt, *The COVID-19 Pandemic Has Become a Catalyst for Cyberattacks*, CSO (Oct. 5, 2020, 2:13 PM), https://www.csoonline.com/article/3584759/the-covid-19-pandemic-has-become-a-catalyst-for-cyberattacks.html.

[7] *Cyberattack*, TECHOPEDIA, https://www.techopedia.com/definition/24748/cyberattack (last updated Feb. 5, 2019).

[8] *See Hacker*, TECHOPEDIA, https://www.techopedia.com/definition/3805/hacker (last updated Dec. 28, 2016) ("[A]ny individual or group that circumvents security to access unauthorized data.").

[9] *Cyberattack*, *supra* note 7.

[10] *See* CISION PR NEWSWIRE, *supra* note 5 (noting that emails from hackers "almost always want you to click on something, for instance to update your payment details, or access the latest information on COVID-19.").

[11] *Cyber losses are increasing in frequency and severity*, HELP NET SECURITY (Sept. 14, 2020), https://www.helpnetsecurity.com/2020/09/14/cyber-losses-are-increasing-in-frequency-and-severity/.

i. Social engineering

Generally, the first step in any cyberattack is a social engineering scam.[12] Social engineering is when a hacker uses psychological manipulation to trick people into divulging private information or performing specific actions.[13] Here, a hacker does not have to force their way in; rather, they convince someone to give them access. Social engineering tactics are especially successful during times of chaos.[14] Recently, hackers used social engineering to access several high-profile Twitter accounts and collected $121,000 in bitcoin.[15] Tom Robinson, co-founder of Elliptic, the cryptocurrency compliance firm that investigated the incident, confirmed the hack involved a Twitter insider.[16] However, it was not a distraught Twitter employee who helped facilitate the hack. Rather, hackers tricked or "socially engineered" the employee to turn off certain security measures, which gave them the ability to access the accounts.[17]

---

[12] "Ninety-eight percent of cyberattacks rely on social engineering." *See 2020 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends*, PURPLESEC, https://purplesec.us/resources/cyber-security-statistics/#:~:text=98%25%20of%20cyber%20attacks%20rely,schemes%20in%20the%20last%20year (last visited Nov. 5, 2020).

[13] *Id.*

[14] *See* CISION PR NEWSWIRE, *supra* note 5 ("'Cybercriminals thrive on chaos, whether it's real or perceived…'" which can lead to "'an uptick in phishing attacks as a result of the global Coronavirus pandemic.'" (quoting Robert Herjavec, founder and CEO at Herjavec Group)).

[15] Kif Leswing, *Twitter hackers who targeted Elon Musk and others received $121,000 in bitcoin, analysis shows*, CNBC (July 16, 2020, 4:25 PM), https://www.cnbc.com/2020/07/16/twitter-hackers-made-121000-in-bitcoin-analysis-shows.html.

[16] *Id.*

[17] *Id. See also* Sheera Frenkel et al., *A Brazen Online Attack Targets V.I.P. Twitter Users in a Bitcoin Scam*, N.Y. TIMES, (May 5, 2021), https://www.nytimes.com/2020/07/15/technology/twitter-hack-bill-gates-elon-musk.html (noting Twitter's internal investigation revealed several employee accounts were compromised). Frenkel noted the accounts became compromised in a "coordinated social engineering attack," an attack "that trick[s] people into giving up their credentials"). *Id.*

Hackers, controlling the verified official Twitter accounts, tweeted: "I am giving back to my community due to COVID-19! All Bitcoin sent to the address below will be sent back doubled."[18] Hackers accessed 130 accounts and the private messages of 36 accounts, including the communications of a Dutch elected official.[19] While hackers seemed to earn a relatively low amount for the historic hack, the incident illustrates the enormous risk social engineering poses to the global economy. According to market experts, by controlling the Twitter accounts of Fortune 500 CEOs, the hackers had the power to manipulate the stock market.[20]

ii. Ransomware

The most chronic cyberattack form is ransomware,[21] which has "reached epidemic proportions."[22] Ransomware is a type of malicious software "designed to gain unauthorized access" to a system.[23] Hackers take a system and "any confidential or sensitive information hostage until the [victim] agrees to pay for its release."[24] Ransomware attacks usually start with social engineering or phishing scams, where an employee unwittingly clicks on a link that contains the ransom malware.[25] The ransomware then encrypts—or holds captive—the corporate victim's data

---

[18] *See* Leswing *supra* note 15 (quoting Former President Barak Obama's official Twitter account).

[19] Kif Leswing, *Twitter says hackers accessed direct messages of 36 victims, including one elected official*, CNBC (July 22, 2020, 8:52 PM), https://www.cnbc.com/2020/07/22/twitter-hack-direct-messages-accessed-including-elected-official.html.

[20] *Id.* This was evidenced by numerous stock price changes to Tesla's and other companies' stock directly correlated with Elon Musk's tweets. *Id.*

[21] *2021 Ransomware Statistics, Data, & Trends*, PURPLESEC, https://purplesec.us/resources/cyber-security-statistics/ransomware/#General (last visited Nov. 18, 2020).

[22] John Reed Stark, *Ransomware's Dirty Little Secret: Most Corporate Victims Pay*, LAW360 (Feb. 6, 2019, 2:21 PM), https://www.law360.com/articles/1123819/ransomware-s-dirty-little-secret-most-corporate-victims-pay.

[23] Stacie L. Lamb & Diana E. McCarthy, *SEC Warns Industry: Remain Vigilant of Cyberattacks*, NAT'L L. REV. (Aug. 11, 2020), https://www.natlawreview.com/article/sec-warns-industry-remain-vigilant-cyberattacks.

[24] *Id.*

[25] Stark, *supra* note 22.

and computer systems.[26] Ransomware attackers threaten to expose the corporate victims' data, unless they pay the ransom, usually with cryptocurrency.[27] Ransomware can devastate a company by locking up an entire corporate network, "encrypting everything from shared drives and email servers to website platforms and backup servers."[28]

An example of ransomware is the infamous Sony hack. North Korean hackers held Sony Pictures' data for ransom, but instead of requesting cryptocurrency, they demanded Sony never release the film, *The Interview*.[29] Sony canceled the theatrical release "amid threats to moviegoers" but still released the film online to various platforms.[30] In response, hackers publicized sensitive data, including thousands of email exchanges, which caused Sony quite the embarrassment and scandal.[31]

The FBI encourages victims to not pay the ransom and instead report the crime to their local FBI office.[32] Paying the ransom encourages and incentivizes ransom hackers to continue their apparently successful work and encourages others to commit the same crime.[33] The FBI's advice leaves corporate victims with a difficult decision, but ultimately, paying the ransom is almost always the least costly option.[34]

---

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] Michael Balsamo & Eric Tucker, *North Korean programmer charged in Sony hack, WannaCry attack*, PBS (Sept. 6, 2018, 2:16 PM), https://www.pbs.org/newshour/nation/north-korean-programmer-charged-in-sony-hack-wannacry-attack.

[30] *Id.*

[31] *Id.* An exchange between Amy Pascal, then co-chairman of the studio, and *The Social Network* producer Scott Rudin was leaked. *Id.* In the exchange, they joked about what might be former President Barack Obama's favorite movies, listing *12 Years a Slave* and films by black comedian Kevin Hart. *Id.* Pascal left her job months later. *Id.*

[32] *Scams and Safety: Ransomware*, FBI, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware (last visited Nov. 4, 2020).

[33] *Id.*

[34] *See* Renee Dudley, *The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks*, PROPUBLICA (Aug. 27, 2019, 5:00 AM), https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks.

Thus, insurance companies will often advise their clients to pay the ransoms because it is less expensive than the costs associated with rebuilding networks, backup recovery, and prolonged operational downtime.[35] The average ransom is $133,000,[36] yet businesses lose "around $8,500 per hour due to ransomware-induced downtime."[37] Moreover, Coveware, which assists victim companies settle cyber extortion events[38], reported "in Q4 2019, victims who paid a ransom to receive decrypting software successfully decrypted 97% of their encrypted data."[39] However, critics argue cyber insurance is keeping ransomware alive.[40] Even more troubling is the emerging Ransomware-as-a-Service (RaaS) technology, which allows cybercriminals to sell/rent ransomware code "to other cybercriminals who have the intent to launch an attack."[41]

iii. Business email compromise, COVID phishing scams, & island-hopping

Business Email Compromise (BEC) is a cyberattack committed with brainpower and manipulation rather than with computer expertise, where a hacker uses social engineering to convince an employee to perform a specific action.[42] A BEC scam starts with an email that appears

---

[35] *Id.*

[36] *See* Leswing, *supra* note 15.

[37] *Id.*

[38] *About Coveware*, COVEWARE, https://www.coveware.com/about (last visited Feb. 24, 2020).

[39] Andrea Tinianow, *Bitcoin Demand Drives $1.4 Billion Ransomware Industry In The U.S.*, FORBES (Jul. 1, 2020, 12:13 PM), https://www.forbes.com/sites/andreatinianow/2020/07/01/bitcoin-demand-drives-14-billion-ransomware-industry-in-the-us/?sh=4dbed8cc32d8.

[40] *See* Dudley, *supra* note 34 (quoting Fabian Wosar, chief technology officer for anti-virus provider Emsisoft, who describes cybercrime and insurance as a "perverted relationship").

[41] Chandra Shekhar Choudhary, *Ransomware-as-a-Service (RaaS): How It Works*, TRIPWIRE (May 16, 2018), https://www.tripwire.com/state-of-security/security-data-protection/ransomware-service-raas-works/.

[42] *See What is Business Email Compromise (BEC)? How Does it Work?*, TESSIAN, (July 13, 2021) https://www.law360.com/articles/1123819/ransomware-s-dirty-little-secret-most-corporate-victims-pay (describing BEC scams as "social engineering attacks").

to be from a trusted source, making a legitimate request, like a vendor emailing an invoice.[43]

Before COVID-19, bad actors rarely used BEC scams for financial gain, but now, the scam is "one of the most financially damaging online crimes."[44] BEC scams were particularly popular with cyber criminals during the COVID-19 pandemic because of their low-tech and low-cost nature.[45] Further, BEC scams carry minimal risk while allowing hackers to successfully exploit urgent and uncertain environments, such as the COVID-19 pandemic.[46] During the pandemic, a typical BEC scam would demand money, couple this demand with an "unexplained urgency," and then blame the pandemic for such a demand outside the normal course of business.[47] For example, the elevated need for personal protective equipment (PPE) during the pandemic was an ideal situation for a BEC scammer.[48] Cyber criminals would impersonate PPE vendors, and, if possible, impersonate an entity that had an existing business relationship with the victim company.[49] Given the short supply of medical equipment, victims were willing to wire money immediately without verifying the seller's information.[50]

The FBI predicted BEC scammers will continue to exploit the pandemic and urges businesses to look out for the following red flags:

> (1) unexplained urgency; (2) last-minute changes in wire instructions or recipient account information; (3) last-minute changes in established communication platforms or e-mail account addresses; (4) communications only in

---

[43] *Scams and Safety: Business Email Compromise*, FBI, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/business-email-compromise (last visited Nov. 1, 2020).

[44] *Id.*

[45] *FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic*, FBI (April 13, 2020), https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic.

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *Id.*

> email and refusal to communicate via telephone or online voice or video platforms; (5) requests for advanced payment of services when not previously required; and (6) requests from employees to change direct deposit information.[51]

Further, CrowdStrike reports in April 2020 alone, the pandemic caused "a 10,000% increase" in coronavirus-themed phishing scams.[52] Bad actors created COVID-19-themed emails with fraudulent "infection maps" and donation links to provide PPE to first responders that appear to come from the CDC or WHO.[53] When successful, the phishing scams provided hackers access to business networks, where they could then "Island Hop."[54] Island-hopping is a form of attack where hackers move "through a supply chain—starting at a weak link—with the overall goal of reaching a connected financial institution."[55] Thus, it is imperative that a company's business partners have strong security measures in place to protect all connected parties from potential data breaches.

For example, the Accellion December 2020 cyberattack illustrates the dangers a company can be exposed to when connected to a "weak link." Accellion is a cloud based security software company which aims to assist businesses in safely and securely communicating sensitive content in the workplace.[56] One of its legacy services, File Transfer

---

[51] *FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic*, FBI, (April 6, 2020), https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic.

[52] Reported by CrowdStrike, an American cybersecurity technology company. *See* Jessica Lyons Hardcastle, *McAfee, CrowdStrike, Palo Alto Networks Track Evolving COVID-19 Cyberattacks*, SDXCENTRAL (May 11, 2020, 10:12 AM), https://www.sdxcentral.com/articles/news/mcafee-crowdstrike-palo-alto-networks-track-evolving-covid-19-cyberattacks/2020/05/ (discussing CrowdStrike's efforts to track COVID-19 related cyberattacks).

[53] *Id.*

[54] Charlie Osborne, *COVID-19 Blamed for 238% Surge in Cyberattacks Against Banks*, ZDNET (May 14, 2020, 11:59 AM), https://www.zdnet.com/article/covid-19-blamed-for-238-surge-in-cyberattacks-against-banks/.

[55] *Id.*

[56] *About Us*, ACCELLION, https://www.accellion.com/company/ (last visited Feb. 24, 2021).

Appliance (FTA) software, was an industry first for providing "a simple way to share large files."[57] Accellion's FTA software was created before the current, more commonly used cloud-based products, like Dropbox and Google Drive.[58] Thousands of companies and government organizations across the world still use FTA software to store and transfer large, sensitive files and emails.[59]

As FTA code aged and Accellion developed newer and more secure products, vulnerabilities developed in the FTA software.[60] In general practice, as was the case here, security researchers will find vulnerabilities in a software and privately report it to the company.[61] However, in December 2020, a cybercriminal exploited an FTA vulnerability and stole data files stored on the software.[62] In January, Accellion confirmed the data breach and stated it patched the vulnerability "within 72 hours to the less than 50 customers affected."[63] On February 1, 2021, however, Accellion admitted the breaches "continued into January 2021."[64]

Among the victims of the FTA cyberattack was the Kroger Company, which disclosed fewer than 1% of customers' data might have been affected but also noted compromised information included employee, pharmacy, and clinic customers' data—including possibly

---

[57] Catalin Cimpanu, *Accellion to Retire Product at the Heart of Recent Hacks*, ZDNET (Feb. 11, 2021, 8:57 PM), https://www.zdnet.com/article/accellion-to-retire-product-at-the-heart-of-recent-hacks/.

[58] *Id.*

[59] *Id.* It is unclear how many organizations currently still utilize the outdated FTA software. *Id.*

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] *Accellion Responds to Recent FTA Security Incident*, ACCELLION, (Jan. 11, 2021), https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/accellion-fta-p0-statementfinal.pdf.

[64] *Press Release Accellion Provides Update to Recent FTA Security Incident*, ACCELLION, (Feb. 1, 2021), https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/.

Social Security numbers.[65] Kroger was notified the FTA hack affected its data on January 23, 2021, nearly a week after Accellion's initial press release.[66] Other victims of the FTA hack "include the University of Colorado, Washington State's auditor, Australia's financial regulator, the Reserve Bank of New Zealand, and the prominent U.S. law firm Jones Day."[67]

Unfortunately, for Washington State's auditor, the hack exposed data from a 2020 investigation on massive unemployment fraud.[68] As for Jones Day, cybercriminals are seeking to extort the law firm and released nearly eighty-five gigabytes of stolen data online.[69] In February 2021, Accellion announced it would terminate its FTA software "a 20 year old product nearing end-of life"[70] because it wants "to move its existing FTA customers over to [its] modern and more secure platform."[71]

---

[65] Zack Budryk, *Kroger Warns Pharmacy Customers' Personal Data May Have Been Stolen in Hack*, THE HILL (Feb. 22, 2021, 8:46 AM), https://thehill.com/policy/cybersecurity/539825-kroger-warns-pharmacy-customers-personal-data-may-have-been-stolen-in.

[66] *Id.*

[67] Frank Bajak, *Kroger Says Pharmacy Customer Personal Data Impacted in Vendor Hack*, 10WBNS https://www.10tv.com/article/news/nation-world/kroger-latest-victim-of-software-data-breach/507-a6348ad4-ae3f-4d3a-8240-1b6e7b96caf5 (last updated Feb. 21, 2021, 3:43 PM).

[68] *Id.*

[69] *Id.*

[70] *Press Release Accellion Provides Update to Recent FTA Security Incident*, ACCELLION, (Feb. 1, 2021), https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/. *See also* Lawrence Abrams, *Data breach broker selling user records stolen from 26 companies*, BLEEPING COMPUTER (Dec. 31, 2020, 10:04 AM), https://www.bleepingcomputer.com/news/security/data-breach-broker-selling-user-records-stolen-from-26-companies/ (describing an example of a large data breach involving brokers); Frequently Asked Questions: General, Bitcoin, https://bitcoin.org/en/faq#general (last visited on Feb. 24, 2021) (outlining Bitcoin and its many uses).

[71] *FTA End of Life*, ACCELLION, https://www.accellion.com/sites/default/files/resources/fta-eol.pdf (last visited on Feb. 24, 2021).

iv. Hackers are not the only culprit

Hackers tend to receive all the notoriety of a cyberattack, however there is another culprit: data breach brokers and cryptocurrencies. Hackers work with data breach brokers who will market and sell the stolen data on behalf of the hackers on dark web marketplaces.[72] In a 2014 study, the Federal Trade Commission (FTC), found individual data brokers retained 1.4 billion records on US citizens.[73] Market experts expect "the market to grow by 11.5 percent yearly through 2022."[74] On Christmas Day in 2020, a data breach broker began selling 368.8 million user records stolen from twenty-six companies.[75] One of those companies was Aurora Cannabis, a Canadian cannabis producer which operates numerous "cannabis-related medical and consumer brands."[76] The hacker "claims to have stolen 50GB of data, including customers' and employees' personal information" and claims "they still have access to Aurora's network."[77]

Additionally, Bitcoin and other cryptocurrencies are enabling the growing economy of the ransomware industry.[78] Bitcoin is currently the most popular and prominent digital cryptocurrency.[79] Bitcoin is the first

---

[72] Abrams, *supra* note 70.

[73] Anouk Ruhaak, *Data Brokers Are Cruising for a Bruising*, WIRED, (Dec. 5, 2019, 9:00 AM), https://www.wired.com/story/opinion-data-brokers-are-cruising-for-a-bruising/.

[74] *Id.*

[75] Abrams, *supra* note 70.

[76] Lawrence Abrams, *Hacker sells Aurora Cannabis files stolen in Christmas cyberattack*, BLEEPING COMPUTER, (Jan. 7, 2021, 5:29 PM), https://www.bleepingcomputer.com/news/security/hacker-sells-aurora-cannabis-files-stolen-in-christmas-cyberattack/.

[77] *Id.*

[78] *See* John Reed Stark, *Ransomware's Year-End Thank You Note To Bitcoin*, LAW360 EXPERT ANALYSIS (Jan. 9, 2020), https://plus.lexis.com/api/permalink/428f6a9c-cfdf-4a9b-93d3-dc3275efe0cf/?context=1530671 (noting Bitcoin is "not just growing in size," but it has also "dramatically expanded the scope" of its business model).

[79] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN, https://bitcoin.org/bitcoin.pdf (last visited Feb. 24, 2021). *See also Frequently Asked Questions: Economy*, BITCOIN, https://bitcoin.org/en/faq#what-if-someone-bought-up-all-the-existing-bitcoins (last visited Sep. 17, 2020) ("Bitcoin remains by far the most popular decentralized virtual currency, but there can be no guarantee that it will retain that position.").

peer-to-peer payment network using money that is completely digital.[80] Since its inception, Bitcoin is notorious for being "the common currency of the Dark Web."[81] In fact, Bitcoin accounts for ninety-eight percent of ransomware payments.[82] It is perfect for ransomware because it is pseudonymous and it allows quick fund transfer funds.[83] Bitcoin states it has "an acceptable level of privacy" but is no more anonymous than using cash.[84] Each Bitcoin transaction is "encrypted with public key cryptography that masks the real identities of the individuals behind the transactions."[85] Each user is assigned two digital keys: (1) a public key that is "published on the bitcoin blockchain, and (2) a private key, which is only known to the user and is the user's 'signature.'"[86] The public blockchain record reflects the time and place of a transaction that occurred "between two public keys (an identifier of [thirty-four] random alphanumeric characters)."[87] Thus, while it is possible to trace bitcoins back to individuals, the process is extremely difficult, expensive, and time consuming.[88]

---

[80] *Frequently Asked Questions: General*, BITCOIN, https://bitcoin.org/en/faq#general (last visited on Feb. 24, 2021).

[81] *Ransomware: Paying Cyber Extortion Demands in Cryptocurrency*, MARSH & MCCLENNAN COMPANIES, https://www.marsh.com/content/dam/marsh/Documents/PDF/US-en/ransomware-cryptocurrency.pdf (last visited on Feb. 24, 2021).

[82] *Id.*

[83] *See id*. ("Why bitcoin? Anonymity. Speed. Access. Bitcoin, like other cryptocurrencies, allows cybercriminals to receive funds with a high degree of anonymity, making transactions difficult to track.").

[84] *Frequently Asked Questions: General*, BITCOIN, https://bitcoin.org/en/faq#general (last visited on Feb. 24, 2021).

[85] Tyler G. Newby & Ana Razmazma, *An Untraceable Currency? Bitcoin Privacy Concerns*, FINTECH WEEKLY, (Apr. 7), https://fintechweekly.com/magazine/articles/an-untraceable-currency-bitcoin-privacy-concerns.

[86] *Id.*

[87] *Id.*

[88] *See id*. ("[B]itcoin is not as untraceable as encryption may imply. Tying an encrypted transaction to an actual individual is possible . . . ."). *See also* Sara Morrison, *What you need to know about ransomware the future of cyberattacks*, VOX (June 16, 2021, 2:45 PM), https://www.vox.com/recode/22527272/ransomware-cyberattacks-bitcoin-explained. Further:

Ciaran Martin, the U.K.'s former cybersecurity chief, stated companies are funding organized crime by paying these ransoms.[89] Making matters worse, companies are filing insurance claims for the ransoms and getting cash back, thus perpetuating the continuity and success of the industry.[90] Her suggested solution is to update existing U.K. extortion laws that currently forbid ransom payments to terrorists but do not apply to ransomware demands.[91]

In the United States, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) warned companies they might face economic sanctions for making ransomware payments to cybercriminals.[92] The Treasury Department acknowledged that ransomware attacks have increased because of the COVID-19 pandemic, but stated making ransomware payments only "encourage[s] future ransomware payment demands."[93] Included on the Treasury Department's sanction list are: two Iranian nationals linked to the SamSam ransomware, North Korea's state-sponsored Lazarus group linked to the WannaCry attack, and Russian cybercriminal organization, Evil Corp, responsible for "the Dridex botnet

---

> Bitcoin, as a global decentralized digital currency, made it much easier for criminals to collect ransom payments and harder for authorities to trace . . . . Ransoms were paid, the attackers got away with them, and over time and with more money, they've evolved into sophisticated criminal enterprises, offering ransomware-as-a-service to partners and creating what some experts liken to franchises. *Id.*

[89] Tanzeel Akhtar, *Former UK Cybersecurity Chief Says Laws Are Needed to Stop Ransomware Payouts*, COINDESK, (Jan. 25, 2021, 1:43 AM), https://www.coindesk.com/former-uk-cybersecurity-chief-says-laws-needed-to-stop-ransomware-pay-outs.

[90] *Id.*

[91] *Id.*

[92] Lucian Constantin, *US Treasury Department ban on ransomware payments puts victims in tough position*, CSO, (Oct. 22, 2020, 5:48 AM), https://www.csoonline.com/article/3587108/us-treasury-department-ban-on-ransomware-payments-puts-victims-in-tough-position.html; *see also OFAC Ransomware Advisory: Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, DEPT. OF TREASURY, (Oct. 1, 2020), https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf [hereinafter *OFAC Ransomeware Advisory*].

[93] *OFAC Ransomware Advisory*, *supra* note 92.

and the WastedLocker and BitPaymer ransomware programs."[94]Anti-malware firm, Emsisoft, has been urging the government to ban ransomware payments because they are "a risk to national security, to election security, to companies' intellectual property and financial security, to individuals' personal information and to their health, safety, and wellbeing."[95]

However, critics argue sanctions will only punish the victim and make already debilitating cyberattacks much more costly.[96] CEO of threat intelligence firm GroupSense, Kurtis Minder, calls the advisory opinion "tone deaf."[97] Minder argued, punishing ransomware victims facing the possibility of going out of business from the ransomware demand alone will drive the market underground.[98]

B. *Cyberattacks Exacerbated by COVID*

In the background of the Coronavirus pandemic is a cybercrime pandemic.[99] According to the FBI, COVID-19 caused a 400% increase in cybercrimes and hacking attacks against U.S. corporations has doubled.[100] For example, in June 2020, new ransomware attacked American companies, thought to be the work of Evil Corp, demanding millions of dollars in ransom.[101]

---

[94] Constantin, *supra* note 92.

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] *Id.*

[99] David Cripps, *Tackling the cybercrime pandemic in 2021*, SECURITY (Sept. 21, 2021) https://www.securitymagazine.com/articles/96134-tackling-the-cybercrime-pandemic-in-2021.

[100] Ryan Smith, *FBI sees a 400% increase in reports of cyberattacks since the start of the pandemic*, INS. BUS. AM. (Aug. 27, 2020), https://www.insurancebusinessmag.com/us/news/cyber/fbi-sees-a-400-increase-in-reports-of-cyberattacks-since-the-start-of-the-pandemic-231939.aspx.

[101] Alex Hern, *Ransomware attack on Garmin thought to be the work of 'Evil Corp'*, THE GUARDIAN (Jul. 27, 2020, 1:57 PM) https://www.theguardian.com/technology/2020/jul/27/ransomware-attack-on-garmin-thought-to-be-the-work-of-evil-corp.

In 2019, before the pandemic, manufacturing was the most targeted global industry sector for cyberattacks.[102] However, during the pandemic, nearly a third of all cyberattacks targeted "either banks or the healthcare sector."[103] "[F]inancial organizations experienced a massive uptick in cyberattack attempts," directly correlated with "pinnacles in the news cycle."[104] When the United States reported its first COVID-related death, cyberattacks increased by nearly 75%.[105]

Fernando Ruiz Pérez, acting head of Europol's Cybercrime Center, states hackers are adapting their methods and causing "a serious threat to life" by targeting healthcare organizations.[106] In October of 2020, the FBI warned hospitals "of an increased and imminent cybercrime threat."[107] FireEye Inc., a cybersecurity company, confirmed a successful and coordinated ransomware attack by "UNC1878, an Eastern European financially motivated threat actor . . . deliberately targeting and disrupting U.S. hospitals."[108] UNC1878 uses ransomware on hospitals to take their networks offline and exploit the urgency to get a quick payout.[109]

A different hacking group, also using ransomware, attacked more than 400 hospitals in the U.S.[110] In one instance, a ransomware attack forced hospital staff at 250 U.S. facilities "to rely on paper and pencil"

---

[102] Joseph Johnson, *Global industry sectors most targeted by cyber espionage in 2019*, STATISTA, (May 29, 2020), https://www.statista.com/statistics/221293/cyber-crime-target-industries/.

[103] Osborne, *supra* at note 54.

[104] *Id.*

[105] *Id.*

[106] Catherine Stupp, *Hackers Change Ransomware Tactics to Exploit Coronavirus Crisis*, THE WALL ST. J., (May 14, 2020, 9:27 AM), https://www.wsj.com/articles/hackers-change-ransomware-tactics-to-exploit-coronavirus-crisis-11589448602.

[107] William Turton, *U.S. Hospitals Warned of Hacking Threat Amid 'Coordinated' Ransomware Attack*, TIME (Oct. 29, 2020 3:27 PM EDT), https://time.com/5905352/hospital-hacking-ransomware/.

[108] *Id.* Russian hackers sent a mysterious postcard to FireEye's CEO after he exposed the breach. *See also* Christopher Bing, *Exclusive: FBI probes Russian-linked postcard sent to FireEye CEO after cybersecurity firm uncovered hack*, REUTERS (Jan. 11, 2021, 12:12 PM), https://www.reuters.com/article/global-cyber-fireeye/exclusive-fbi-probes-russian-linked-postcard-sent-to-fireeye-ceo-after-cybersecurity-firm-uncovered-hack-sources-idUSL1N2JM1Q9.

[109] Turton, *supra* note 107.

[110] *Id.*

which forced them to divert patients to other providers.[111] That same month, in Germany, a hospital was forced to reroute a critically ill patient to a different city after "an IT system failure."[112] Unfortunately, the patient became "the first known fatality related to ransomware."[113]

In March 2020, in what is being labeled as "the worst-ever [U.S.] government cyberattack," hackers used ransomware and the "supply chain" infiltration tactic, to target "America's nuclear weapons arsenal," and powerful tech and security companies, including Microsoft.[114] While Donald Trump, then President of the United States, dismissed the hack, federal officials stated the attack "posed a 'grave risk' to every level of government" while investigators are still trying to determine what information might have been stolen.[115]

Hackers managed to sneak malicious code into "updates to a popular software called Orion" which "provides network-monitoring and other technical services to hundreds of thousands of organizations around the world, including most Fortune 500 companies and government agencies in North America, Europe, Asia and the Middle East."[116] The malicious code allowed hackers "remote access" to steal information from the organization's networks.[117] Hackers had access to the networks for months which gave them "ample opportunity to extract" email and other internal communications.[118] The attack "compromised at least nine federal agencies and 100 private companies" including some of the world's largest

---

[111] *US hospital systems facing 'imminent' threat of cyber-attacks, FBI warns*, THE GUARDIAN (Oct. 29, 2020 12:44 AM), https://www.theguardian.com/society/2020/oct/28/us-healthcare-system-cyber-attacks-fbi.

[112] *Id.*

[113] *Id.*

[114] Kari Paul & Lois Beckett, *What we know – and still don't – about the worst-ever US government cyber-attack*, THE GUARDIAN (Dec. 19, 2020, 2:57 PM), https://www.theguardian.com/technology/2020/dec/18/orion-hack-solarwinds-explainer-us-government.

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *Id.*

IT vendors[119] and dozens of other security and technology firms.[120] The number and location of victims continues to grow as the investigation unfolds.[121] SolarWinds, the company who created Orion, reported 45% of its total revenue was affected and its "stock price has fallen 25% since news of the breach first broke."[122]

Cyber-conflict expert, Thomas Rid, states it is likely hackers "harvested such a vast quantity of data" they likely do not realize what information might be useful yet.[123] While then-Secretary of State, Mike Pompeo, publicly confirmed the attack was linked to Russia, a Kremlin spokesperson has stated: "One shouldn't unfoundedly blame the Russians for everything," to which Trump agreed.[124] Cybersecurity experts state the federal government must do more to stay "up to date on cybersecurity issues."[125] Experts suggest one possible quick fix would be to reinstate the "positions of White House cybersecurity coordinator and state department cybersecurity policy chief," which the Trump administration had eliminated.[126]

In February 2021, almost one year later, SolarWinds CEO, Sudhakar Ramakrishna, spoke publicly for the first time about the hack.[127] Ramakrishna stated they have learned two things: (1) they are still learning the "breadth and depth of the sophistication of the attackers" and (2) the attackers were patient and persistent evidenced by their use of early

---

[119] Dustin Volz, *More SolarWinds Hack Victims Yet to Be Publicly Identified, Tech Executives Say*, THE WALL ST. J. (Feb. 23. 2021 7:50 PM), https://www.wsj.com/articles/senate-panel-probes-solarwinds-hack-to-learn-how-big-how-broad-hit-was-11614086918.

[120] Paul & Beckett, *supra* note 114.

[121] *Id.*

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] *Id.*

[126] Paul & Beckett, *supra* note 114.

[127] "Ramakrishna took over as CEO weeks after news about the hack of SolarWinds' updates to its Orion software had become public." *See* Tim Starks, *SolarWinds CEO talks hack, remaining questions before Capitol Hill hearings*, CYBERSCOOP (Feb. 22, 2021), https://www.cyberscoop.com/solarwinds-sudhakar-ramakrishna-ceo-hack/ (discussing the steps SolarWinds was taking in the aftermath of the attack).

versions of Orion code "as a test bed for their eventual attack."[128] He "wishe[d]" there was a centralized location to report breaches that could then be shared across sectors and governments.[129] Additionally, on February 23, at the Senate Intelligence Committee hearing, Microsoft President Brad Smith, FireEye CEO Kevin Mandia, and CrowdStrike President and CEO George Kurtz, along with several senators—all agreed that "Congress needs to pass a clear national data breach notification law."[130]

Mandia, CEO of FireEye, the cybersecurity firm that first identified the attack, wondered if they had not come forward "would we still be in the dark?"[131] Microsoft President, Brad Smith, complained contractual obligations restricted them from notifying other agencies after it discovered the SolarWinds breach.[132] He further highlighted the deeper issue that companies are not typically legally compelled to disclose breaches, thus the scope of the attack was impossible to determine.[133] He suspected "other brand-name players" may have been compromised but are keeping "customers in the dark."[134] Senate Intelligence Chairman Mark Warner, D-VA criticized Amazon's absence from the hearing, implying it had also suffered an intrusion "but left the public in the dark."[135]

C. *"Safer at Home" Except Against Cyberattacks*

In 2018, Department of Homeland Security Secretary, Kirstjen Nielsen, warned "[Cyberspace] is now the most active battlefield" with attacks extending "into almost every American home" moving "past

---

[128] *Id.*

[129] *Id.*

[130] Tim Starks, *Senate hearing on SolarWinds hack lays bare US shortcomings, remaining mysteries*, CYBERSCOOP (Feb. 23, 2021), https://www.cyberscoop.com/solarwinds-fireeye-microsoft-crowdstrike-senate-ssci/.

[131] *Id.*

[132] Volz, *supra* note 119.

[133] *Id.*

[134] *Id.*

[135] *Id.*

the 'epidemic' stage" becoming a "pandemic."[136] In March 2020, almost one-third of the human population was under some form of lockdown during the COVID-19 pandemic.[137] "Stay-at-home" orders forced many businesses to shift their employees to remote work. Although individuals were "safer at home," businesses became perfect targets for cyberattacks.[138] The *H1 2020 Cyber Insurance Claims Report* found cybercriminals are taking advantage of organizations' new technology supporting the transition of remote work.[139]

For example, employees working from home likely use a virtual private network to log into their company's network. According to the Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), this sharp increase in VPN usage creates vulnerabilities in these systems for "malicious cyber actors" to exploit.[140] Additionally, businesses with overwhelmed information technology departments are struggling to secure their databases as "[d]ata leaks due to carelessness [are] on the rise[.]"[141] Sometimes, data leaks are a direct result of businesses failing to simply password-protect their databases.[142]

---

[136] Breanne Deppisch, *DHS Was Finally Getting Serious About Cybersecurity. Then Came Trump.*, POLITICO (Dec. 18, 2019, 5:06 AM), https://www.politico.com/news/magazine/2019/12/18/america-cybersecurity-homeland-security-trump-nielsen-070149.

[137] Mia Jankowicz, *More People Are Under Lockdown Now than Were Alive During World War II*, BUS. INSIDER (Mar. 25, 2020, 8:36 AM), https://www.businessinsider.com/more-people-under-lockdown-than-alive-during-world-war-ii-2020-3.

[138] *Hacking against corporations soars as staff work from home*, E&T, (Apr. 17, 2020), https://eandt.theiet.org/content/articles/2020/04/hacking-against-corporations-surges-as-people-work-from-home/.

[139] Finding "exploitation of remote access was the root cause of reported ransomware incidents." AIT News Desk, *Coalition Releases New Report on Cybersecurity Claims Trends Amid COVID-19*, AITHORITY (Sept. 14, 2020), https://aithority.com/security/coalition-releases-new-report-on-cybersecurity-claims-trends-amid-covid-19/.

[140] E&T, *supra* at note 138 (quoting the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency).

[141] Scott Ikeda, *Major Data Broker Exposes 235 Million Social Media Profiles in Data Leak: Info Appears to Have Been Scraped Without Permission*, CPO MAG., (Aug. 28, 2020), https://www.cpomagazine.com/cyber-security/major-data-broker-exposes-235-million-social-media-profiles-in-data-leak/.

[142] *Id.*

II. CYBERATTACKS AND THE LAW

A. *Businesses as Victims – 18 U.S.C. § 1030*

In 1986, Congress enacted the Computer Fraud and Abuse Act (CFAA) as the first federal computer fraud law.[143] Congress intended to address "in a single statute the problem of computer crime."[144] The CFAA states that "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished" by fine or imprisonment.[145] Additionally, "[w]hoever . . . with intent to extort . . . any money or other thing of value," communicates a "threat to cause damage . . . to obtain [or] to impair the confidentiality of information obtained" will violate the CFAA.[146]

i. The CFAA is breathtakingly broad

First, as defined by statute, a "protected computer" is any computer "used in or affecting interstate or foreign commerce or communication[.]"[147] Courts broadly interpret a "protected computer" as virtually anything connected to the internet.[148] Second, a defendant must "obtain" information, which is misleading because mere observation of data is sufficient.[149] Finally, the access must be intentional and either without authorization or exceeding authorized access.[150] The United States Supreme Court has yet to interpret the CFAA, leaving the lower courts to

---

[143] 18 U.S.C. § 1030; *Computer Fraud and Abuse Act (CFAA)*, NACDL, https://www.nacdl.org/Landing/ComputerFraudandAbuseAct (last visited Nov. 1, 2020).

[144] S. REP. NO. 104-357, at 5 (1996) (Conf. Rep.).

[145] 18 U.S.C. § 1030(a)(2)(C).

[146] 18 U.S.C. § 1030(a)(7)(A)–(B).

[147] 18 U.S.C. § 1030(e)(2)(B).

[148] *See* United States v. Nosal (Nosal I), 676 F.3d 854, 859 (9th Cir. 2012); United States v. Kramer, 631 F.3d 900, 902 (8th Cir. 2011) (defining "computer" as "any device that makes use of an electronic data processor," including a cell phone); United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (holding a website is a computer).

[149] S. REP. NO. 99-432, at 6 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2484.

[150] *Id.*

define its broad terms. Courts interpret "access" broadly, finding access when logging onto a computer,[151] sending or receiving an email,[152] or extracting data from a web site.[153] Further, "although the CFAA does not define 'authorization,' courts have found the term 'clear' and given it a 'straightforward meaning.'"[154] For instance, the Ninth Circuit has consistently interpreted "authorization" to mean "permission or power granted by an authority."[155]

a. *Unauthorized access versus exceeding authorization*

Since Section 1030(e) does not define "without authorization" or unauthorized access, courts must interpret the words as taken in "their ordinary, contemporary, common meaning."[156] Courts find access "without authorization" to mean accessing "a computer without any permission at all."[157] Therefore, a defendant violates the CFAA if they do not have permission to access a computer or if the employer explicitly revokes such permission.[158] For example, the Ninth Circuit, in *Facebook, Inc. v. Power Ventures, Inc.*, held permission was "expressly rescinded" where Facebook, sent a cease and desist letter to Power Ventures, putting

[151] United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010).

[152] Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1273 (N.D. Iowa 2000); s*ee also* Shawn E. Tuma, *"What Does Cfaa Mean and Why Should I Care?"—A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. Rev. 141, 172 (2011).

[153] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579, 581–82 (1st Cir. 2001).

[154] Sandvig v. Barr, 451 F. Supp. 3d 73, 84–85 (D.D.C. 2020) (quoting United States v. Nosal (Nosal II), 844 F.3d 1024, 1035 (9th Cir. 2016)).

[155] LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009).

[156] *Id.* at 1132–33 (quoting Perrin v. United States, 444 U.S. 37, 42 (1979) (internal quotation marks omitted)).

[157] LVRC Holdings LLC v. Brekka, 581 F.3d at 1133.

[158] Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016); *see also* LVRC Holdings LLC v. Brekka, 581 F.3d at 1136 (reasoning where a former employee uses work credentials to access and obtain information about the former employer, former employee would have done so without authorization); *see also* hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1003 (9th Cir. 2019) ("[W]hen a computer network generally permits public access to its data, a user's accessing that publicly available data will not constitute access without authorization under the CFAA.").

them on notice that they no longer have authorization to access its network.[159]

The Seventh Circuit in *International Airport Centers, LLC v. Citrin*, applying agency law, held where an employee breaches his duty of loyalty to his employer, his authorization to access a work computer terminates.[160] In *Citrin*, before the employee resigned, he loaded "a secure-erasure program" to his work computer designed to permanently delete all of its data.[161] In doing so, the *Citrin* court, held the defendant violated the CFAA because "his authorization to access the laptop terminated when he engaged in misconduct that violated [his] duty of loyalty."[162] Accordingly, the Seventh Circuit held the employee's actions were "without authorization."[163]

In *LVRC Holdings LLC v. Brekka*, however, the Ninth Circuit held an employee had authorization to send work documents to his personal email because he had permission to access his work computer.[164] In both *Brekka* and *Citrin* the employees had authorization to access their company computers and left their employment to start competing businesses.[165] However, the *Brekka* court declined to adopt the *Citrin* interpretation because the "plain language of the statute" indicates that authorization "depends on actions taken by the employer," and to interpret it otherwise would not give defendants notice of criminal liability.[166]

b. *Authorization: to access or for usage?*

Both *Brekka* and *Citrin* illustrate that the difference between "without authorization" and "exceeding authorized access" is paper-thin.[167] "Exceeds authorized access," as defined in Section 1030(e)(6), "means to access a computer with authorization," and use such access "to obtain or alter information . . . the accesser is not entitled to obtain or

---

[159] *Facebook*, 844 F.3d at 1067.
[160] Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006).
[161] *Citrin*, 440 F.3d at 419.
[162] *Id.* at 420.
[163] *Id.* at 421.
[164] LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009).
[165] *Id.* at 1134; Citrin, 440 F.3d at 419.
[166] *Id.* at 1135.
[167] *Citrin*, 440 F.3d at 420.

alter."[168] The Ninth Circuit defines "without authorization" as without permission, however, "a person who 'exceeds authorized access'" does so with permission to access the computer, but accesses information they are not entitled to access.[169] This holding limits exceeding authorization to *access* restrictions, not *use* restrictions.[170] In *Brekka*, the employee did not violate the CFAA when he sent confidential emails to himself and his wife because he was authorized to access those documents, in addition to the computer.[171] The Ninth Circuit adopted a narrow view, holding the CFAA applies to employees who unlawfully *access* a protected computer, but not to the improper *use* of information lawfully accessed.[172]

Other circuits have refused to interpret the language this narrowly leading to a circuit split. The Seventh Circuit, in *Citrin*, held the broader view that "when employees access computer information with the intent to harm their employer, their authorization to access that information terminates, and they are therefore acting 'without authorization.'"[173] The Eleventh Circuit, in *United States v. Rodriguez*, held where an employee accessed personal information for "nonbusiness reasons" he violated the CFAA.[174] The Ninth Circuit, en banc in *Nosal II*, declined to follow that interpretation because activities like playing games, shopping, or watching sports highlights would become federal crimes.[175] The Fifth Circuit in *John*, added an additional layer, holding if an employee's use of information is criminal, they exceed their authorized access.[176]

c. *United States v. Van Buren*

Thus, to address the circuit split, the Supreme Court granted certiorari in *Van Buren v. United States* to resolve whether a person who is authorized to access information on a computer for specific purposes

---

[168] 18 U.S.C. § 1030(e)(6).

[169] *LVRC Holdings*, 581 F.3d at 1133.

[170] United States v. Nosal (Nosal I), 676 F.3d 854, 854 (9th Cir. 2012).

[171] *LVRC Holdings*, 581 F.3d at 1129, 1137.

[172] United States v. Steele, 595 F. App'x 208, 211 (4th Cir. 2014) (referencing WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199 (4th Cir.2012) (citing United States v. Nosal, 676 F.3d 854, 863 (9th Cir.2012) (en banc)).

[173] Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).

[174] 628 F.3d 1258, 1263 (11th Cir. 2010).

[175] *Nosal II*, 676 F.3d at 860 (en banc).

[176] United States v. John, 597 F.3d 263, 271 (5th Cir. 2010).

violates Section 1030(a)(2) if they access the same information for an improper purpose.[177] In *United States v. Van Buren*, a Georgia police officer accepted $6,000 in exchange for information gleaned from running a license plate number.[178] Officer Van Buren fostered a relationship with Andrew Albo, a sixty-year-old man who often ran into trouble with the law for soliciting prostitutes.[179] Van Buren regularly "handled the disputes between Albo and various women," even though the Deputy Chief of Police believed Albo to be "very volatile" and have "a mental health condition."[180]

On August 21, 2015, Albo gave Van Buren $5,000 in exchange for information on a woman he met at a strip club who he thought might be an undercover officer.[181] Unbeknownst to officer Van Buren, but true to Albo's character, Albo recorded their conversation and reported Van Buren to law enforcement, which drew FBI involvement.[182] On August 31, Albo gave officer Van Buren "a fake license plate number created by the FBI" and an additional $1,000.[183] Two days later, on September 2, officer Van Buren accessed the Georgia Crime Information Center (GCIC) database and searched for the license-plate number.[184] The next day, the FBI arrested Van Buren who was later charged and convicted on one count of felony computer fraud in violation of 18 U.S.C. § 1030.[185]

On appeal before the Eleventh Circuit, Van Buren argued he only accessed "'databases he was authorized to use,' albeit for inappropriate

---

[177] Deborah F. Buckman, *Annotation, Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A § 1030)*, 174 A.L.R. Fed. 101 (Originally published in 2001); Van Buren v. United States, 140 S. Ct. 2667 (2020).

[178] United States v. Van Buren, 940 F.3d 1192 (11th Cir. 2019).

[179] *Id.* at 1197.

[180] *Id.*

[181] *Id.*

[182] *Id.*

[183] *Id.* at 1198. "The FBI gave Albo $2,000 to pass to Van Buren, so it appears Albo may have attempted to retain $1,000 for himself." *Id.* at 1198 n.2.

[184] *Id.* at 1198.

[185] *Id.* Van Buren was also charged with one count of honest-services wire fraud, in violation of 18 U.S.C. §§ 1343 and 1346. *Id.* The Eleventh Circuit vacated this conviction based on erroneous jury instructions and remanded for a new trial. *Id.* at 1210.

reasons."[186] As the court noted, this argument was effectively an appeal to overrule its decision in *United States v. Rodriguez*.[187] Ultimately, the Eleventh Circuit held it was bound to follow *Rodriguez*, "under our prior-precedent rule," because "no Supreme Court or en banc decision of this Circuit . . . abrogates *Rodriguez*."[188] Therefore, because the GCIC database "is supposed to be used for law-enforcement purposes only" and Van Buren accessed the database to investigate a woman in exchange for $6,000 "under [their] binding Circuit precedent," the court affirmed Van Buren's CFAA conviction.[189]

As discussed earlier, and as mentioned by the *Van Buren* Court, other circuits "have criticized the *Rodriguez* interpretation of "exceeds authorized access."[190] The Supreme Court's decision in *Van Buren* will determine "whether millions of ordinary Americans are committing a federal crime" whenever they engage in common computer activities that violate the terms of use of their employer or online service.[191]

ii. Ambiguous verbiage & non-ally defendants add to the complexity

Congress intended for the Computer Fraud and Abuse Act (CFAA) to provide "law enforcement with the necessary legal framework to fight computer crime."[192] Thus far, Congress has succeeded somewhat, however, the "CFAA is breathtakingly broad"[193] creating "conflicting

---

[186] *Id.* at 1207.

[187] *Id.*

[188] *Id.* at 1208.

[189] *Id.*

[190] *Id.*

[191] Zack Whittaker, *The Supreme Court will hear its first big CFAA case*, TECHCRUNCH, (Nov. 29, 2020, 6:00 AM), https://techcrunch.com/2020/11/29/supreme-court-van-buren-hacking/.

[192] S. Rep. No. 104–357, pt. II. *See also* Deborah F. Buckman, *Annotation, Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030)*, 174 A.L.R. Fed. 101 (2001) (explaining Congress' intentions).

[193] *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1577 (2010) (noting the CFAA's broadness "is the heart of the problem").

interpretations among the various federal courts of appeal."[194] Additionally, cyberattacks perpetrated from outside the United States by Russia, China, and Iran, for example, "pose an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States."[195] Although it is arguably ineffective in deterring such attacks, the punishment for cyberattacks perpetrated by non-ally countries is most often sanctions.[196] For example, the United States has attributed many cyberattacks to the Russian government, yet it was not until 2020 when the U.S. brought its first criminal charges against named Russian intelligence officers.[197]

B. *Businesses as the Defendant – CCPA § 1798.50*

The California Consumer Privacy Act (CCPA), enacted in 2018, is the first privacy bill of its kind in the United States.[198] A business that is the victim of a cyberattack becomes the defendant, under the CCPA and could face fines of thousands of dollars where personal information is breached.[199] CCPA Section 1798.150 allows for a private right of action for consumers to file suit against a business that failed to implement and maintain reasonable security procedures and practices causing nonencrypted and nonredacted personal information to be "subject to an unauthorized access and exfiltration, theft, or disclosure."[200] A consumer must provide the violating business with thirty-days' notice before filing a civil suit.[201] If the business cures the violation and provides written notice

---

[194] Shawn E. Tuma, *"What Does Cfaa Mean and Why Should I Care?"- A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141, 154 (2011).

[195] Cyber Deterrence and Response Act of 2019, 116 H.R. 1493.

[196] *Id.*

[197] *Id. See also Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace*, US. DEP'T OF JUST. (Oct. 19, 2020) https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[198] Devin Coldewey, *The California Consumer Privacy Act officially takes effect today*, TECHCRUNCH, (Jan. 1, 2020, 6:01 AM), https://techcrunch.com/2020/01/01/the-california-consumer-privacy-act-officially-takes-effect-today/.

[199] *Id.*

[200] 2020 Cal. Stat. § 1798.150(a)(1).

[201] 2020 Cal. Stat. § 1798.150(b).

within thirty days, the consumer can no longer file suit.[202] Recovery is guaranteed at a minimum of $100 per consumer per incident and can exceed the established ceiling of $750 if actual damages are greater.[203] Additionally, a consumer could seek injunctive or declaratory relief.[204] A court can also grant any other relief it "deems proper."[205] This past November, Californians approved Prop 24, the California Privacy Rights Act (CPRA), in order to strengthen their existing privacy protections by building on the CCPA.[206] The updated measure becomes effective on January 1, 2023, and makes minor changes to Section 1798.150.[207]

i. Nonencrypted and nonredacted personal information

Under the CCPA, the information at issue must be personal.[208] Personal information (PI), as defined in Section 1798.81.5(d)(1)(A), is an individual's first name or first initial and the individual's last name in combination with a social security number or other identifiers.[209]

Second, the PI must be nonencrypted and nonredacted.[210] Interestingly, both terms only appear once throughout the entire statute, and neither are defined.[211] The plain meaning of "nonencrypted" is data that has not been translated "into another form, or code, so that only people with access to a secret key or password can read it."[212] However, "nonredacted" is not as plainly defined in the technology or legal community. Redaction is "the permanent removal of information and not

---

[202] *Id.*

[203] 2020 Cal. Stat. § 1798.150(a)(1)(A).

[204] 2020 Cal. Stat. § 1798.150(a)(1)(B).

[205] 2020 Cal. Stat. § 1798.150(a)(1)(C).

[206] Sara Morrison, *Live Results for California's Data Privacy Ballot Initiative*, VOX, https://www.vox.com/policy-and-politics/2020/11/3/21546835/california-proposition-24-live-results-data-privacy (last updated Nov. 4, 2020).

[207] CA Prop. 24 (2020), 2020 Cal. Legis. Serv. Prop. 24 (PROPOSITION 24) § 1798.150(a)(1) (West).

[208] 2020 Cal. Stat. § 1798.81.5(a)(1) (West).

[209] 2020 Cal. Stat. § 1798.81.5(d)(1)(A)–(B) (West).

[210] 2020 Cal. Stat. § 1798.150(a)(1).

[211] *See generally* Cal. Civ. Code § 1798.150 (West).

[212] Nate Lord, *What is Data Encryption? Definition, Best Practices, & More*, DIGITAL GUARDIAN, (Dec. 1, 2020), https://digitalguardian.com/blog/what-data-encryption.

the obscuring of it."[213] However, in the situation triggered by § 1798.150, nonredacted PI would be nearly all data retained by a business because it has not been "removed" from their database. This interpretation does not align with the CCPA's intent because various other sections address precisely how and why a business can store PI.[214] Legislators should define these terms in future amendments because the ambiguity will lead to litigation, as we have seen with the CFAA's verbiage.[215]

ii. Comparing the CCPA to § 1030(g) of the CFAA

The Computer Fraud and Abuse Act (CFAA) provided only criminal penalties until the Computer Abuse Amendments Act of 1994.[216] Now, the CFAA provides a private right of action for "[a]ny person who suffers damage or loss by reason of a violation of this section."[217] Under § 1030(g), the corporation is the victim since its computers were violated, made inaccessible, or damaged.[218] Thus, the hackers are liable under the CFAA. However, in that same scenario, under the CCPA, the consumer is the victim since the hacker accessed their information.[219] Thus, businesses, not cybercriminals, are liable under the CCPA.

Additionally, § 1030(g) has more restrictions than the CCPA.[220] First, § 1030(g) requires that the conduct involve one of the four factors included in § 1030(c)(4)(A)(i).[221] The first and most common factor is "loss to [one] or more persons during any [one]-year period," and the plaintiff is limited to economic damages.[222] The CCPA does not limit a

---

[213] *Redaction*, TECHOPEDIA, https://www.techopedia.com/definition/30529/redaction (last visited Nov. 4, 2020).

[214] *See, e.g.*, 2020 Cal. Stat. § 1798.100 (describing how businesses should properly collect, store, use, and sell PI, as well as when businesses are required to disclose the collection of PI).

[215] *See supra* Section II.A.

[216] Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1066 (9th Cir. 2016).

[217] 18 U.S.C. § 1030(g).

[218] *Id.*

[219] 2020 Cal. Stat. § 1798.150(a)(1).

[220] *Compare* 18 U.S.C § 1030(g), with 2020 Cal. Stat. § 1798.150(a)(1).

[221] 18 U.S.C § 1030(g).

[222] § 1030(c)(4)(A)(i)(I).

victim to economic damages in any case, let alone cases involving loss.[223] Second, the complaint must be brought within two years of the violation or the discovery of damage date.[224] While the CCPA requires a consumer to give notice to the violator, it does not impose a statute of limitation.[225]

iii. The CCPA is vague, yet still too narrow

In addition to the vagueness of the statute, there are other flaws within the CCPA. First, Section 1798.150 does not cover all ransomware attack scenarios. Ransomware attacks are unique because victims never lose possession of their data; they lose *access* to it.[226] Yet under Section 1798.150, an individual can only bring a lawsuit in a situation where their PI was subject to unauthorized "exfiltration, theft, or disclosure."[227]

For example, before COVID-19, hackers infiltrated business networks and spent time inspecting the data to determine if the information was valuable enough to move forward with the ransom.[228] Now, hackers are targeting businesses they know "need [their] data back right away," like hospitals or "compan[ies] operating online more than before" because of COVID restrictions.[229] Thus, it is possible hackers will not view any personal information, let alone exfiltrate, steal, or disclose it. A ransomware attack is like a burglar who breaks into a home but does not steal anything. Instead, the burglar changes the locks and requires the homeowner to pay a fee to receive the new keys. If a business fails to pay the ransom and hackers subsequently release private information to the public, then a consumer may file suit against the business. If a business pays the ransom and hackers do not exfiltrate, steal, or disclose the data, however, a patient at one of these hospitals would not be able to file suit under the CCPA.[230]

---

[223] 2020 Cal. Stat. § 1798.150(a)(1).
[224] 18 U.S.C § 1030(g).
[225] 2020 Cal. Stat. § 1798.150(a)(2)(b).
[226] Stark, *supra* at note 22.
[227] 2020 Cal. Stat. § 1798.150.
[228] Stupp, *supra* at note 106.
[229] *Id.*
[230] *Id.*

III. THE EXECUTIVE BRANCH'S CYBERSECURITY APPROACH: TRUMP V. BIDEN

While the judicial branch is busy hopefully cleaning up the circuit split the CFAA's broad language created, the executive branch has introduced two very different approaches to cybersecurity during the COVID-19 pandemic.

A. *The Trump Administrations' Cybersecurity Legacy*

Unfortunately, the Trump Administration did little to progress cybersecurity. In fact, the Trump Administration demoted cybersecurity as a policy field by "discontinu[ing] the Cybersecurity Coordinator position at the White House, shr[inking] the State Department's cyber diplomacy wing, and by fir[ing] federal cybersecurity leader Chris Krebs in the aftermath of Donald Trump's Nov. [sic] 3 election defeat."[231]

First, according to Debora Plunkett, a former NSA official who is now a fellow at Harvard University's Belfer Center, "[e]liminating the White House cyber-coordinator role was a step in the wrong direction."[232] Longtime NSA official Rob Joyce filled the top cyber official position tasked with "developing policy to defend against increasingly sophisticated digital attacks and the use of offensive cyber weapons."[233] In

---

[231] Christopher Bing & Joseph Menn, *After big hack of U.S. government, Biden enlists 'word class' cybersecurity team*, REUTERS (Jan. 22, 2021, 3:09 AM), https://www.reuters.com/article/us-usa-biden-cyber/after-big-hack-of-u-s-government-biden-enlists-world-class-cybersecurity-team-idUSKBN29R18I.

[232] Joseph Marks, *The Cybersecurity 202: Trump took the nation in the wrong direction on cybersecurity, experts say*, THE WASHINGTON POST (Dec. 15, 2020), https://www.washingtonpost.com/politics/2020/12/15/cybersecurity-202-trump-took-nation-wrong-direction-cybersecurity-experts-say/.

[233] Nicole Perlroth & David E. Sanger, *White House Eliminates Cybersecurity Coordinator Role*, THE NEW YORK TIMES (May 15, 2018), https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html; *See also* Shannon Vavra, *Rob Joyce named new NSA cybersecurity director*, CYBERSCOOP (Jan. 15, 2021), https://www.cyberscoop.com/rob-joyce-nsa-cybersecurity-director-neuberger/. The Biden Transition Team has announced Rob Joyce will replace Anne Neuberger as the new NSA Cybersecurity director. *Id.* Neuberger will join the

response, Congress mandated in a recent defense policy bill, "creating an even more powerful White House cyber-director position" which Trump threatened to veto if confirmed by the Senate.[234]

Ultimately, it was the firing of Christopher Krebs, former director of the Cybersecurity and Infrastructure Security Agency (CISA), that produced the most damage.[235] Trump himself appointed former Director for Cybersecurity Policy for Microsoft, Chris Krebs, to lead CISA.[236] But, it was Krebs' success and leadership in combatting cyber threats and 2020 election misinformation which severed their relationship.[237] Trump fired Krebs by tweet in October 2020 after CISA "signed on to a statement vouching for the integrity of the 2020 election."[238] President Trump's tweets read:

> The recent statement by Chris Krebs on the security of the 2020 Election was highly inaccurate, in that there were massive improprieties and fraud - including dead people voting, Poll Watchers not allowed into polling locations, "glitches" in the voting machines which changed. . . votes from Trump to Biden, late voting, and many more. Therefore, effective immediately, Chris Krebs has been terminated as Director of the Cybersecurity and Infrastructure Security Agency.[239]

Biden Administration as deputy national security adviser for cyber and emerging technology on the National Security Council (NSC). *Id.*

[234] Marks, *supra* at note 232.

[235] *Id.*

[236] *Christopher C. Krebs*, CISA, https://www.cisa.gov/christopher-c-krebs (last visited Feb. 24, 2021).

[237] Alex Scroxton, *US cyber security chief fired for contradicting Trump*, COMPUTERWEEKLY (Nov. 18, 2020, 12:00 AM), https://www.computerweekly.com/news/252492286/US-cyber-security-chief-fired-for-contradicting-Trump.

[238] Marks, *supra* at note 232.

[239] Noah Y. Kim, *Fact-checking Donald Trump's tweet firing Christopher Krebs*, POLITIFACT (Nov. 18, 2020), https://www.politifact.com/factchecks/2020/nov/18/donald-trump/fact-checking-donald-trumps-tweet-firing-christoph/; *see also* ARCHIVE.TODAY, (Nov. 18, 2020), https://archive.is/1gN5x/image (quoting the former President's tweets) Please note, the two tweets are separated by the ellipsis and included within the same quote because they were nearly simultaneous and the second tweet is a continuation of the thought started in the first.

Additionally, under Krebs, CISA launched a "Rumor Control" website which debunked "phony election fraud claims, including some propagated by the president."[240] Former NSA official Steve Ryan stated, "[f]rom a cybersecurity policy and operations standpoint, firing Chris Krebs, Tom Bossert, and Rob Joyce have put our nation in peril at a time when we need cyber-protection the most."[241] Jake Williams, a former National Security Agency hacker and the founder of Rendition Infosec, stated, "Krebs was one of those individuals that was widely trusted outside the government. His firing is likely to reduce the trust shown by the private sector to the government regarding cybersecurity."[242]

In December 2020, Congress progressed cybersecurity when it passed the Internet of Things (IOT) Cybersecurity Improvement Act of 2020, which established "minimum security standards for [IOT] devices owned or controlled by the Federal Government."[243] The bill enjoyed rare bipartisan support, with Democrats and Republicans being represented almost equally.[244] While the bill only regulates federal IOT devices, experts are hopeful that, as manufacturers create federal complaint devices, the safer devices will trickle into the private sector for consumers as well.[245]

Some experts found the Trump Administration's actions to be in the right direction. Megan Stifel, an Obama White House cybersecurity official, "praised CISA for 'building trust and capacity with the election community,'" though noted "credit should rest with the heads of the organizational entities."[246] Stewart Baker, a former NSA general counsel,

---

[240] Marks, *supra* note 232.

[241] *Id.*

[242] *Id.*

[243] IoT Cybersecurity Improvement Act, H.R.1668, 116th Cong. (2020) (enacted).

[244] Deborah George, *New Federal Law Alert: The Internet of Things (IoT) Cybersecurity Improvement Act of 2020 – IoT Security for Federal Government-Owned Devices*, THE NATIONAL LAW REVIEW (Dec. 10, 2020), https://www.natlawreview.com/article/new-federal-law-alert-internet-things-iot-cybersecurity-improvement-act-2020-iot.

[245] Knud Lasse Lueth, *IoT 2020 in Review: The Most Relevant IoT Developments of the* Year, IOT ANALYTICS (Jan. 12, 2021), https://iot-analytics.com/iot-2020-in-review/.

[246] Marks, *supra* note 232.

commended the Trump Administration for "turning CISA into a real cybersecurity agency with an effective role in protecting the 2020 election and imposing significant new sanctions on Russia."[247] Steve Grobman, chief technology officer at McAfee, celebrated the Trump Administration's creation of CISA, but found the firing of Krebs to be a "setback[]" for cybersecurity.[248] Paul Rosenzweig, a top DHS official during the George W. Bush administration who now runs Red Branch Consulting, applauded CISA's "support of election security."[249] However, Paul noted that government officials made such progress "despite the resistance of Trump himself and the wrongheaded decision of Trump/Bolton to de-emphasize cybersecurity at the NSC level."[250]

B. *The Biden Administration's Cybersecurity plan*

Since taking office in 2021, President Joe Biden has launched an "urgent initiative" to improve the nation's cybersecurity.[251] First, the President created a new position of Deputy National Security Advisor for Cyber and Emerging Technology.[252] Second, while describing the "nation's cybersecurity as a 'crisis,'" Biden's COVID-19 recovery proposal allocated more than $10 billion to "cyber security and information technology."[253] Third, President Biden said he made it clear in a conversation with Russian President Vladimir Putin "in a manner very different from [his] predecessor" that he would not "roll[] over in the face of aggressive actions."[254]

Cybersecurity experts praised the Biden Administration's choice of Anne Neuberger for the new position of Deputy National Security

---

[247] *Id.*
[248] *Id.*
[249] *Id.*
[250] *Id.*
[251] Maggie Miller, *Biden: US taking 'urgent' steps to improve cybersecurity*, THE HILL (Feb. 4, 2021, 5:24 PM), https://thehill.com/policy/cybersecurity/537436-biden-says-administration-launching-urgent-initiative-to-improve-nations.
[252] *Id.*
[253] *Id.*
[254] *Id.*

Adviser for Cyber and Emerging Technology.[255] Neuberger rose to fame for her work at the NSA's cyber defense wing where she "dr[ew] praise for quickly alerting companies to hacking techniques in use by other countries."[256] The Biden Administration claims it will be taking a collaborative approach "to national security" and promises to work closely with "the private sector to protect against threats to the American people."[257] Appointing Neuberger seems to be a positive first step in that direction because she "is well respected within the cybersecurity community."[258] Further, Neuberger herself has pledged to improve the currently poor sharing practices of the Agency.[259]

Microsoft corporate Vice President Tom Burt applauded the Biden Administration for "appoint[ing] world-class cybersecurity experts to leadership positions."[260] However, others are worried "the collective group's experience is almost entirely in the public sector."[261] Former (DHS) Cybersecurity Director, Amit Yoran, who now serves as CEO of security company Tenable, Inc., warns a good balance between "government and commercial experience will be critical to success."[262] Additionally, the Biden Administration's current plan seems to focus solely on national cybersecurity and does not yet address a specific plan to confront cyberattacks specifically against American businesses. This is unfortunate because American businesses continue to be targeted and victimized by cybercriminals.

---

[255] Tonya Riley, *The Cybersecurity 202: NSA cyber chief Anne Neuberger is heading to the Biden White House*, THE WASHINGTON POST (Jan. 14, 2021), https://www.washingtonpost.com/politics/2021/01/14/cybersecurity-202-nsa-cyber-chief-anne-neuberger-is-heading-biden-white-house/.

[256] Bing & Menn, *supra* note 231.

[257] Mariam Baksh, *Biden Team Snatches NSA Cyber Chief for White House Role*, NEXTGOV (Jan. 13, 2021), https://www.nextgov.com/cybersecurity/2021/01/biden-team-snatches-nsa-cyber-chief-white-house-role/171384/.

[258] *Id.*

[259] *Id.*

[260] Bing & Menn, *supra* note 231.

[261] *Id.*

[262] *Id.*

IV. THE FUTURE OF CYBERSECURITY

A. *Minor Changes that Could have Major Impact*

First, aside from updating and clarifying the statutory language of the CFAA and CCPA mentioned earlier, the United States could also implement regulations similar to proposed legislation in the European Union that requires businesses to work with technology services that maintain strict security standards.[263] Regulators would have the power to terminate "contractual agreements with technology providers" if they failed "to fix cybersecurity problems identified in government inspections."[264] Similar legislation in the United States could effectively ensure businesses are taking the right step towards increased cybersecurity. However, if providing legislatures with the power to terminate private contracts is too intrusive, instead, the United States could impose fines on noncompliant businesses and still reach the desired effect of increased cybersecurity.

Second, the United States could implement penalties for businesses that pay ransoms following a ransomware attack. As explained above, for most businesses, paying the ransom is the least costly option.[265] However, substantial penalties would render the option to pay the ransom costlier.[266] Businesses are more likely to implement greater security when facing a hefty fine.[267] Imposing fines against a victim, however, may be unfair and may not make a dent in "the dramatic growth of ransomware."[268] Third, the United States could more frequently add cybercriminals to terrorist lists.[269] This would afford the United States

---

[263] Catherine Stupp, *EU Seeks Authority to Cut Off Banks' Tech Suppliers if Found Wanting on Cybersecurity*, WALL ST. J. (Oct. 6, 2020, 5:30 am ET), https://www.wsj.com/articles/eu-seeks-authority-to-cut-off-banks-tech-suppliers-if-found-wanting-on-cybersecurity-11601976601.

[264] *Id.*

[265] *See* discussion *supra* Section I.A.2.

[266] Stark, *supra* note 22.

[267] *See* Silvia Amaro, *EU Announces Sweeping New Rules that Could Force Breakups and Hefty Fines for Big Tech*, CNBC (Dec. 15, 2020, 11:56 AM EST), https://www.cnbc.com/2020/12/15/digital-markets-act-eus-new-rules-on-big-tech.html. Amaro notes, an EU official hopes hefty fines will result in "practical changes rather than fining those breaching the rules constantly." *Id.*

[268] Stark, *supra* note 22.

[269] *Id.*

access to international cooperation, greater resources for investigations, intelligence-gathering, and prosecution efforts.[270]

Fourth, the Federal Bureau of Investigation (FBI) could partner with a growing number of private-sector companies entering the market as "ransomware payment facilitators."[271] These incident response firms help businesses negotiate with ransomware attackers and can attempt to recover lost data.[272] These firms can also "construct a payment scheme" where payment is delivered only upon receipt of the encryption key.[273] Often, a business is more likely to hire a digital forensics firm to help maneuver the ransomware attack than it is to contact the FBI.[274] These digital forensics firms, acting as mediators, gain access to an onslaught of evidence, information, and resources. While it is not the FBI's role to mediate a crime, it could create partnerships with these firms to gain access to that crucial evidence. This type of open communication could lead to more prosecutions. Further, it is crucial for the online community to work together and communicate to counter cybercrime.

When working to mitigate the harm of cybercrime, it is important to keep in mind two problems: (1) jurisdictional issues make prosecution of overseas cybercriminals difficult,[275] and (2) large companies can afford to lobby for cybersecurity legislation and can also afford to stay compliant, while small businesses cannot.[276] One of the major problems with bringing

---

[270] UNITED NATIONS OFFICE ON DRUGS AND CRIME, THE USE OF THE INTERNET FOR TERRORIST PURPOSES (2012), https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf.

[271] Stark, *supra* note 22.

[272] *Id.*

[273] *Id.*

[274] *Id.*

[275] *See* UNITED NATIONS OFFICE ON DRUGS AND CRIME, *supra* note 270, at 96–98.

[276] *See* James Rundle & David Uberti, *Cybersecurity Lobbying Spending Mounts as Privacy, Security Laws Take Shape*, WALL ST. J. (May 4, 2020, 3:07 PM), https://www.wsj.com/articles/cybersecurity-lobbying-spending-mounts-as-privacy-security-laws-take-shape-11588619239. *See also Stay Safe from Cybersecurity Threats*, SMALL BUS. ADMIN., https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats (last visited Sept. 23, 2021).

cybercriminals to justice is the struggle to enforce existing law.[277] "[F]or every 1,000 cyber incidents," only three receive an enforcement response.[278] "Malicious cyber actors outside the U[nited]S[tates] are acting with impunity, and, understandably, fear no consequences from the harm they impose on Americans."[279] Additionally, large companies, like Microsoft and Facebook, can afford to spend $1 billion a year on cybersecurity.[280] However, few companies have the resources to spend anywhere near that and yet face the same threats.[281]

B. *Businesses need to Protect & fend for Themselves*

Nearly a decade ago, Robert Mueller, then-Director of the FBI, stated "there are only two types of companies: those that have been hacked and those that will be."[282] Thus, it is imperative that companies initiate proactive measures to ensure they do not become victims or mitigate the damage if they do become one. In May 2017, Representative Tom Graves (R-GA) proposed, in the Active Cyber Defense Certainty Act 2.0., that victims should be able to defend themselves by "hacking back" which is when a cyberattack victim, without authorization, accesses the computer it believes hacked its network. [283] Opposing parties argue this would lead to a chain reaction of legal hacking and thus is not practical nor ideal.[284]

---

[277] Ishan Mehta, *Under Trump, the Fight Against Cybercrime Has Waned*, WIRED (June 20, 2019, 9:00 AM), https://www.wired.com/story/under-trump-the-fight-against-cybercrime-has-waned/.

[278] *Id.*

[279] *Id.*

[280] Klon Kitchen, *A Major Threat to Our Economy – Three Cyber Trends the U.S. Must Address to Protect Itself*, THE HERITAGE FOUND., (Oct. 2, 2019), https://www.heritage.org/cybersecurity/commentary/major-threat-our-economy-three-cyber-trends-the-us-must-address-protect.

[281] *Id.*

[282] Robert S. Mueller, III, *Combating Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies*, FBI (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[283] Active Cyber Defense Certainty Act, H.R. 4036, 115th Cong. § 3 (2017) *See also* Martin Matishak, *Graves goes big on cyber in last days of Appropriations*, POLITICO, (Jul. 17, 2020, 12:05 PM), https://www.politico.com/news/2020/07/17/graves-goes-big-on-cyber-in-last-days-of-appropriations-367712. (defining the term "hacking back").

[284] ORIN S. KERR, COMPUTER CRIME LAW 143 (4th ed. 2018).

Therefore, it is imperative that businesses protect themselves and implement essential internal solutions, like "training and education," to combat cyberattacks.[285] One of the simplest steps a company can take is to invest in antivirus and firewall software, patch management, and password management.[286] The first step every company must take is to have secure hardware that is password-protected, and sensitive information should always further require two-way authentication.[287] Excellent password management does much more than ensure ex-employees cannot access company information after they have been terminated. It is the first step in defense. While cybercriminals have found ways to access password-protected information, having strong and secure passwords makes the task much more difficult, and nearly impossible for the common hacker.[288] Additionally, an efficient password management system can ensure those accessing certain data are authorized to do so via their permissions.[289] Consistent patch management will guarantee there are no vulnerabilities in a company's system that would allow cybercriminals to access company data.[290] Proper patch management could have prevented many of the breaches Accellion experienced.[291]

Safety is especially important now, while employees are working remotely. Another example, firms must store data on secure cloud services instead of the internal computer storage.[292] Data breaches often occur

---

[285] *The Cost of Cybercrime*, ACCENTURE, 9, https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50 (last visited Sep. 19, 2021).

[286] Traci Spencer, *How to Protect Your Business from Cyber Attacks*, NIST, (Oct. 22, 2019), https://www.nist.gov/blogs/manufacturing-innovation-blog/how-protect-your-business-cyber-attacks.

[287] Naveen Goud, *Ways to prevent cyber attacks on your company*, CYBERSECURITY INSIDERS, https://www.cybersecurity-insiders.com/ways-to-prevent-cyber-attacks-on-your-company/ (last visited Feb. 26, 2021).

[288] *The Importance of Strong, Secure Passwords*, SECURE DATA RECOVERY, https://www.securedatarecovery.com/resources/the-importance-of-strong-secure-passwords (last visited Feb. 26, 2021).

[289] *Id.*

[290] *See* Spencer, *supra* note 286.

[291] *See* Cimpanu, *supra* note 57 (noting that Accellion released a firmware patch within 3 days of attacks, but failed to notify their customers and many didn't realize the update was waiting to be applied).

[292] *See* Goud, *supra* note 287.

when employees who have important and sensitive data stored on their computers, lose or have their computer stolen.[293] Additionally, encryption helps companies protect their computers and stored backups by making it harder for cybercriminals to access company data, motivating them to move on to other victims for efficiency.[294] Finally, it is imperative for a company to set up an official procedure which outlines exactly what to do when a cybersecurity incident occurs.[295] Employees must receive up-to-date training on company protocol to ensure the proper steps are taken. [296]

Ultimately, the best protection for a company would be to acquire cyber insurance policies for when the inevitable happens.[297] Cyber insurance helps "mitigate losses from a variety of cyber incidents, including data breaches, business interruption, and network damage."[298] Cyber insurance will become as commonplace as workers' compensation insurance with global premiums "expected to grow from about $2.5 billion to approximately $7.5 billion by next year."[299]

In June of 2019, a ransomware attack locked a Florida city's computer files.[300] Both the city manager and mayor decided to have their cyber insurer, Beazley, pay the bitcoin ransom equivalent to $460,000.[301] Luckily, the city's cyber-insurance policy covered ransomware and thus the city only paid a $10,000 deductible.[302] The mayor stated that while it was an unpleasant decision, paying the deductible would get the city back to business, instead of "spend[ing] money [they] don't have to just get back up and running."[303]

---

[293] *Id.*

[294] *See* Spencer, *supra* note 286.

[295] *Id.*

[296] *Id.*

[297] *See* Goud, *supra* note 287.

[298] *Cybersecurity Insurance*, CISA, https://www.cisa.gov/cybersecurity-insurance (last visited Feb. 25, 2020).

[299] Rich Ehisen, *Data Privacy Laws, Hackers Put New Emphasis on Cyber Insurance*, LEXISNEXIS, https://www.lexisnexis.com/en-us/products/state-net/news/2019/11/01/data-privacy-laws.page (last visited Sep. 22, 2021).

[300] Dudley, *supra* note 34.

[301] *Id.*

[302] *Id.*

[303] *Id.*

Unfortunately, the relationship between cyber insurance and cybercriminals is perverse.[304] Insurance companies will often accommodate attackers' demands instead of pursuing alternative solutions.[305] Both the FBI and various security researchers claim paying ransoms, and in turn cyber insurance companies, are not only fueling cybercrime, but ultimately "funding terrorist regimes."[306] Critics claim cyber insurers will "pay anything, as long as it is cheaper than the loss of revenue they have to cover otherwise."[307] The FBI has reportedly warned that hackers specifically target "American companies that they know have cyber insurance."[308] Loretta Worters, spokeswoman for the Insurance Information Institute, a nonprofit industry group based in New York, explains that cybercriminals realize they have access to the "deep pockets" of insurance companies whose only goal is to get the victim back to business.[309]

"Lloyd's, which underwrites about one-third of the global cyber-insurance market, said that coverage is designed to mitigate losses" and provide expert consulting to help repair damage and fix any weaknesses within the company.[310] Worters admitted the industry does not want to "perpetuate people committing fraud . . . but [sometimes they] are better off paying."[311] Executive Vice President of Solis Security Chris Loehr explained even when backups are available, everyone involved "wants the ransom paid."[312]

Even when companies have backed up their data, it could take a month to restore it from the cloud, whereas paying the ransom to obtain a decryption key is faster.[313] Getting the customer decrypted and minimizing business interruption loss "makes the client happy, it makes the attorneys happy, [and] it makes the insurance happy."[314] Loehr further stated, when clients are morally opposed to paying a ransom demand, he reminds them

---

[304] *Id. See also* discussion *supra* Section I.A.2.
[305] Dudley, *supra* note 34.
[306] *Id.*
[307] *Id.*
[308] *Id.*
[309] *Id.*
[310] *Id.*
[311] *Id.*
[312] *Id.*
[313] *Id.*
[314] *Id.*

of their financial interests.[315] While Loehr conceded, "it sucks having to pay off assholes," the client must remember they could end up "dead in the water" if they continue to suffer interruption loss.[316]

V. CONCLUSION

By 2025, cybercrime will cost the world $10.5 trillion annually and "will be more profitable than the global trade of all major illegal drugs combined."[317] The United States needs to quickly pass clear legislation, including a federal privacy law similar to the CCPA, impose regulations and/or fines for ransomware victims and cyber insurance companies, and work to improve its enforcement mechanisms overseas to protect its citizens, businesses, and the global economy. Otherwise, businesses will remain defenseless, and the global market will suffer. Until then, businesses will need to protect themselves and, in the process, their consumers.

---

[315] *Id.*

[316] *Id.*

[317] Morgan, *supra* note 3. Estimate "is based on historical cybercrime figures including . . . a dramatic increase in hostile nation-state sponsored and organized crime gang hacking activities." *Id.* Further, "[c]ybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm." *Id.*