DATA BREACHES: ARE CHIEF INFORMATION SECURITY OFFICERS NOW IN LEGAL PERIL?

Natalie Kempton*

I. Introduction

Nearly fifteen billion data records have been compromised by cybercriminals in the past decade.¹ Companies’ cybersecurity is at an all-time low as a result of advancements in technology and side effects of COVID-19.² Cybersecurity is the protection of devices, data, and

---

* J.D. Candidate, Suffolk University Law School, 2024.
1 See Ivana Vojinovic, Data Breach Statistics That Will Make You Think Twice Before Filling Out an Online Form, DATAPROT (Jan. 21, 2023), archived at https://perma.cc/Y8HD-SWX6 (pointing out that 14,717,618,286 data records have been compromised in cyber security attacks since 2013).
2 See Rob Sobers, 166 Cybersecurity Statistics and Trends [updated 2022], VARONIS (July 8, 2022), archived at https://perma.cc/8AEN-NUSJ (describing how recent security research shows that many companies do not have adequate cybersecurity practices as COVID-19 increased remote work). “Expanding 5G networks connected devices at faster speeds and greater bandwidths” leading to an increase in cybersecurity breaches. Id. “On average, only five percent of companies’ folders are properly protected.” Id. See also Bernard Marr, The Biggest Cyber Security Risks in 2022, FORBES (Mar. 18, 2022), archived at https://perma.cc/4CLZ-WD8N (discussing how COVID-19 moved our lives “online to cope with lockdowns and restrictions” resulting in “fraudsters hav[ing] enjoyed greater opportunities to strike.”). See also The Importance of Cybersecurity Amid Covid-19, ABA (Oct. 17, 2022), archived at https://perma.cc/7648-5HLA (discussing how “[t]imes of
networks from unlawful use and practice. Cybersecurity is critical because there are many risks that come with poor cybersecurity safeguards, such as data breaches. Data breaches reveal protected or sensitive information and can affect virtually every individual, organization, or corporation who uses any type of technology. According to the 2021 Thales Data Threat Report, 45% of U.S. companies experienced a data breach in 2020. These cybersecurity breaches have a variety of negative repercussions, such as significant financial losses and a lack of trust in essential emerging technology despite technological advancements having the capability to greatly benefit the world we live in.

See also Impact of COVID-19 on Cybersecurity, Deloitte (Oct. 17, 2022), archived at https://perma.cc/U4N9-BWDX (describing how cyber attackers have used the COVID-19 pandemic to increase their illegal cyber activities).

See Security Tip (ST04-001), Cybersecurity & Infrastructure Security Agency (Nov. 2019) (defining cybersecurity). See also Carrie E. Cope et al., Cyber Risks, Social Media and Insurance: A Guide to Risk Assessment and Management § 8, at 1 (2022) (describing laws and regulations that further cybersecurity). Many state governments and regulatory agencies have “enacted legislation designed to ensure that businesses and organizations take appropriate measures to protect themselves and their data.” Id. See also Kevin Cloutier et al., Cybersecurity Measures to Protect Employer’s Confidential Information and Trade Secrets, 1-2 (Lexis Prac. Advisor, 2022) (describing cybersecurity and the benefits it has of “reducing opportunities for unauthorized parties to gain access” to a corporations’ networks).

See U.S. Government Accountability Office, GAO Report Data Breaches 1, 3 (2019) (examining how to handle data breaches). Data breaches are so dangerous to consumers and corporations because personal information can be stolen from consumers for years after data breaches. Id. See Security Tip (ST04-001), supra note 3 (describing risks to having poor cybersecurity). See Gia Snape, Data Breaches are costing more – what companies need to know, Ins. Bus. America (Aug. 22, 2022), archived at https://perma.cc/63BF-3FG2 (explaining how data breaches are costing more every year and that the “global average cost of a data breach in 2022 is $4.35 million, higher by $0.11 million that last year’s cost and the highest to date.”).

See Juliana De Groot, The History of Data Breaches, DataInsider (Aug. 22, 2022), archived at https://perma.cc/SZ84-G4RD (explaining who data breaches affect). Data breaches have existed since individuals and companies have kept private information. Id. See also Sobers, supra note 2 (defining data breaches).

See Aimee O’Driscoll, 30+ data breach statistics and facts, Comparitech (Sept. 16, 2022), archived at https://perma.cc/SH35-VLYF (noting that “[t]he US suffers from the most data breaches” in the world).

See Marr, supra note 2 (describing how trust in technology is key). “[T]echnology and data have the potential to do real good in the world, including solving massive
American Corporations are the most susceptible targets of data breaches and have historically reacted to increasing cyberattacks by creating a stronger emphasis and focus on amplifying cybersecurity as a defense. As a response to breaches, the C-level position of Chief Information Security Officer (CISO) was created and instituted in many companies in the early 2000s. This executive position is designed to hone in on an organization’s security operations, cyber risks, data loss investigations, program management, and governance. CISOs are expected to be a strong leader for company problems like ending the energy crisis, feeding the hungry, protecting the environment, and curing disease.”

However, without trust in tech and data many technological advancements that benefit the greater world are not possible. See also O’Driscoll, supra note 6 (noting that “[c]ompanies that have experienced a breach underperform the market by more than 15% three years later.”). There is a correlation between data breaches and the continuing success of a company. See also IBM Report: Cost of a Data Breach Hits Record High During Pandemic, IBM (July 18, 2021), archived at https://perma.cc/9FRY-JD7J [hereinafter IBM Report] (documenting that data breaches cost corporations an average of $4.24 million). In 2021 data breaches were the most cost worthy in the “17-year history of the [IBM] report.”

The monetary cost of a cyberattack can be potentially devastating due to the financial impact and inoperable hours of company work. See The Importance of Cybersecurity in Business, BBC (Oct. 19, 2022), archived at https://perma.cc/44S7-VTBF (discussing how “[c]ompanies with 250 or more employees were revealed to be more than two times more likely to be targeted for an attack as companies between 10 and 49 employees.”). The position of CISOs is expanding as technology advances and these executives are now taken a “more expansive role in the organization.”

See Josh Fruhlinger, How the CISO role is evolving, CSO (Apr. 1, 2021), archived at https://perma.cc/46HB-K2QU (noting that 80% of large enterprises now have CISOs). The position of CISOs is expanding as technology advances and these executives are now taken a “more expansive role in the organization.” See also What is a CISO?, CISO (Oct. 17, 2022), archived at https://perma.cc/A2TZ-XMPN (describing the difference between a CIO and a CISO). A CISO focuses on the compliance and security of the CIO’s technology implementations.
protection and mitigation of security risks as they work with other executives to establish and maintain ardent security policies.\textsuperscript{11}

Historically, CISOs have not been held legally liable for data breaches or cybersecurity issues that a company sustains.\textsuperscript{12} However, this shield of liability appears to be in jeopardy as the federal government prosecuted and convicted a CISO of a company for concealing a data breach for the first time in \textit{U.S. v. Sullivan}.\textsuperscript{13} \textit{U.S. v. Sullivan} is stirring up the cyber protection community and causing many C-level executives to worry about their potential liability when handling data breaches within their company.\textsuperscript{14} \textit{U.S. v. Sullivan} potentially creates a new precedent that CISOs will be held solely,
legally accountable for their company’s failure to properly handle a data breach.\footnote{See Daniel Garrie, Lessons For Cybersecurity Officers After Ex-Uber Exec Trial, LAW360 (Oct. 12, 2022), archived at https://perma.cc/6TXT-3MLU (pointing out how many CISOs are concerned that \textit{U.S. v. Sullivan} is adding a “further layer of liability” onto an already stressful job). “A CISO might think that now they not only have to deal with the challenges of remediating a data breach, but also risk criminal prosecution if they make a wrong move.” \textit{Id}.}

There is a strong consternation from many CISOs and other security professionals that \textit{U.S. v. Sullivan} initiates a new precedent that encourages the criminal prosecution of CISOs for mishandling data breaches in the past, present, and future.\footnote{See Johana Bhuiyan, Uber’s ex-security chief faces landmark trial over data breach that hit 57m users, GUARDIAN (Sept. 7, 2022), archived at https://perma.cc/D46L-BSRZ (discussing the importance of the \textit{U.S. v. Sullivan} case and potential new standards it could create). “At a time when reports of ransomware attacks have surged and cybersecurity insurance premiums have risen, the case could set an important precedent regarding the culpability of US security staffers and executives for the way the companies they work for handle cybersecurity incidents.” \textit{Id}. See also Cade Metz, Former Uber Security Chief Found Guilty of Hiding Hack from Authorities, N.Y. TIMES (Oct. 5, 2022), archived at https://perma.cc/W5XG-Y6HH (pointing out that \textit{U.S. v. Sullivan} can potentially alter how security professionals handle data breaches). \textit{See Garrie, supra} note 15 (highlighting other CISOs reaction and questions for how this case will affect their previous and future job performance). A former CISO for Coca-Cola Co. and Campbell Soup Co., pointed out that companies usually pick to pay ransom charges when hackers attack and now questions, “[s]ix years from now, will all of them be prosecuted?” \textit{Id}.} This note addresses this apprehension and argues that executives should not be held exclusively liable for data breaches within their companies regardless of when the potential mishandling of the data breach occurred. A company should continue to be the only entity held accountable for data breaches rather than an individual CISO if other executives and employees were aware of the breach. This note will contend that CISOs should especially not be held criminally liable for failing to disclose data breaches because not only do CISOs not have enough control in a company to be held solely accountable for a cybersecurity breach, creating this precedent will also dissuade people from taking CISO roles in the future.\footnote{See Sabin, supra note 14 (discussing how cybersecurity experts are concerned that convicting CISOs could dissuade people from becoming CISOs).}  The government should rather maintain an open line of communication with CISOs and encourage early reporting.
instead of emphasizing the unnerving consequences of mishandling complex data breaches.

II. History

A. The Evolution of Data Breaches

Data breaches were first accounted for over a half-century ago in the 1980s when home computers became commonplace for the average American household. Breaches in the 1980s and 1990s were much less sophisticated, consisting mainly of low-technology hacking engendered primarily by human error or relatively simple computer viruses. Substantial breaches remained a scarcity until the early 2000s when mobile devices and portable computers became a commonality to American society with the expansion of this higher technology. The first major data breach that transpired during this new age of technology in the 2000s was at DSW Shoe Warehouse,

18 See Frank Olito, Computers actually date back to the 1930s. Here’s how they’ve changed., INSIDER (Sept. 13, 2019), archived at https://perma.cc/S9VH-PSU6 (discussing how Apple came out with Macintosh which “was described as a game-changer for the computer industry.”). See De Groot, supra note 5 (noting that data breaches began in the 1980s, but the public was not fully aware of them until the 2000s). “Most information on data breaches focuses on the time period from 2005 to today.” Id. See David Kalat, Nervous System: The First Major Data Breach, 1984, LTN (Dec. 8, 2020), archived at https://perma.cc/X88K-Q9ZX (articulating that the first data breach occurred in 1984 when the credit histories of over 90 million Americans were exposed when a computer password was posted to an electronic board). This is still one of the “largest identity-theft data breaches that the financial services industry has publicly acknowledged.” Id. See also When did Personal Computers Become Popular?, REFERENCE (Apr. 2, 2020), archived at https://perma.cc/D4B2-GRXA (discussing how during the late 1970s and early 1980s computers became affordable for the average American because they were built smaller). Before the late 1970s and early 1980s computers were not practical for home use due to their great size and expense, so they were mainly used for businesses and government organizations. Id.

19 See Keith D. Foote, A Brief History of Data Security, DATAVERSITY (Dec. 29, 2020), archived at https://perma.cc/YUU6-SWME (highlighting the timeline of data breaches from the 1980s to today). “Interest in viruses, particularly malicious viruses, continued to grow . . . in the 1980s and in the 1990s, [v]iruses and hackers were creating chaos at an alarming rate . . . .” Id.

20 See De Groot, supra note 5 (describing how “public awareness of the potential for data breaches began to rise.”). “[T]he advancement of technology and proliferation of electronic data throughout the world, making data breaches a top concern for both enterprises and consumers.” Id.
where over 1.4 million credit card numbers were stolen in 2005. The DSW breach exhibited that the expansion of technology could pose difficulties to companies data security. In spite of DSW’s major cybersecurity catastrophe, many corporations still did not understand or acknowledge the full extent of this technological expansion and the repercussions it could pose to their own companies. Therefore, when the largest data breach to date first occurred in 2013, where hackers took records from all three billion Yahoo accounts, many companies were shocked. The Yahoo breach, in addition to sparking a public interest in breaches and cyber security regulations, also increased awareness in corporations of the heightened risk posed by hackers,

21 See DSW Inc., 052 F.T.C. 3096 (2006) (noting how DSW violated the FTC Act describing the punishment for their violation). See also The Evolution of Data Breaches, CARDCONNECT (Oct. 18, 2022), archived at https://perma.cc/5A2D-88W9 (recognizing that from the first major data breach in 2005 to 2018 there has been “more than 8,790 data breaches in the U.S. [which] have been made public, with more than 11 billion individual records breached.”). Data breaches are mainly caused today by malicious or criminal activity, however human and system error account for the other minority of breaches. Id. See DSW Inc. Settles FTC Charges, FTC (Dec. 1, 2005), archived at https://perma.cc/8NXE-N5XL (describing how DSW agreed to settle with the FTC for “its failure to take reasonable security measures to protect sensitive customer data [which was deemed] an unfair practice that violated federal law.”).

22 See DSW Inc. Settles FTC Charges (describing the DSW breach and its aftermath on the cybersecurity community). The FTC found that “96,000 checking accounts were compromised, and that there have been fraudulent charges on some of these accounts.” Id.

23 See Nadia Damouni, Exclusive: U.S. companies seek cyber experts for top jobs, board seats, REUTERS (May 30, 2014), archived at https://perma.cc/MX3X-MMRU (pointing out how it took almost a decade after major high-profile data breaches for companies to take data breaches seriously).

24 See Michael Hill & Dan Swinhoe, The 15 biggest data breaches of the 21st century, CSO (July 16, 2021), archived at https://perma.cc/CXZ5-QASR (describing the Yahoo attack and how it took years to find out the true number of records that were exposed). However, the hackers only accessed “account information such as security questions and answers” and personal data such as “passwords, payment card and bank data were not stolen.” Id. See also Kayla Matthews, IOTW: Multiple Yahoo data breaches across four years result in a $117.5 million settlement, CYBER SEC. HUB (Oct. 7, 2019), archived at https://perma.cc/V925-PM5G (recalling how Yahoo did not properly respond after the major data breaches). Yahoo settled by paying $117.5 million to 896 million accounts in April of 2019. Id. Yahoo continued to have data security intrusions where information was stolen from 2013 to 2016, however, the company did not immediately disclose these breaches to the public or the FTC. Id.
breaches, and the prospective grim consequences a company could suffer as a result.\textsuperscript{25}

At present, technology is expeditiously expanding, continuously imposing new obligations on companies and their security professionals.\textsuperscript{26} Though companies have recently commenced efforts to expand their data security to protect from cyberhackers, technology is rapidly modernizing, and the multifaceted nature of this growth is proving grueling to combat.\textsuperscript{27} Corporations around the globe saw the aftermath of poor security practices and the diversifying technology field as major companies continue to frequently suffer from cyberattacks despite cyber-defensive actions.\textsuperscript{28} A significant reason for this persistence of attacks is that companies are failing to mitigate risks early on before they pose a major threat to an organization.\textsuperscript{29} Today, it is not enough to simply have an IT

\textsuperscript{25} See Matthews, supra note 24 (discussing the aftereffects of the Yahoo breach). “The aftermath of that event continued for years later, sparking increased public awareness both about these breaches and the respective cyber security laws []” Id. See also Eileen Brown, One in four Americans won’t do business with data-breached companies, ZDNET (Feb. 28, 2020), archived at https://perma.cc/Y8UX-BDJI (listing statistics from a study of customers opinions on companies who have experienced data breaches in 2018).

The findings showed that almost one in four Americans stop doing business with companies who have been hacked, and more than two in three people trust a company less after a data breach. Almost all respondents (92\%) agree that companies are financially liable to their customers after a breach and over one in five people are unwilling to give their financial information to a company who’s been hacked.

\textsuperscript{26} See How technology is changing the security industry, AZBIGMEDIA (July 14, 2020), archived at https://perma.cc/CM66-76M3 (pointing out how advancements in technology breakthroughs causes the security industry to constantly evolve).

\textsuperscript{27} See Benjamin Edwards et al., Hype and heavy tails: A closer look at data breaches, 2 J. CYBERSECURITY 3, 12 (2016) (juxtaposing how even though security practices are improving, attacks have become more sophisticated). “The ability to monetize personal information, and the increasing ease with which financial transactions are conducted electronically could mean that the cost of data breaches will rise in the future.” Id.

\textsuperscript{28} See id. at 13 (discussing the repercussions of data breaches to corporations). “[D]ata breaches pose an ongoing threat to personal and financial security, and they are costly for the organizations that hold large collections of personal data. In addition, because so much of our daily lives is now conducted online, it is becoming easier for criminals to monetize stolen information.” Id.

\textsuperscript{29} See Adam Levin, How Can 73 Percent of Companies Not Be Prepared for Hackers?, INC. (Oct. 24, 2022), archived at https://perma.cc/H5F4-PLSG
department with security protocols; companies now have to take preventative measures in order to stop data breaches and understand a diversity of technology infrastructures. This can pose complications because a variety of new complex infrastructures have been constructed, such as SaaS applications and cloud environments, which aggravate the likelihood of data breaches even when companies intensify their cybersecurity defenses.

See Poremba, supra note 9 (reiterating that it is not enough anymore for companies to rely on the implementation of firewalls and antivirus software). Companies must identify and attenuate threats to have a successful cybersecurity defense. See also Wesley Chai, Software as a Service (SaaS), TECHTARGET (Feb. 21, 2023), archived at https://perma.cc/9L9Z-KEWA (defining a SaaS, or a “[s]oftware as a service”). A SaaS “is a software distribution model in which a cloud provider hosts applications and makes them available to end users over the internet.” See also Nathan Eddy, Data Breaches Rise as Organizations Shift to the Cloud, SEC. BOULEVARD (June 30, 2021), archived at https://perma.cc/7359-XBE9 (pointing out how the multitudes of technology and SaaS applications creates a more difficult heterogenous landscape for companies to defend). See also Ermetic Reports Nearly 100% of Companies Experienced a Cloud Data Breach in Past 18 Months, ERMETIC (June 23, 2021), archived at https://perma.cc/TZ3N-DPYT (noting that cloud infrastructure security company, Ermetic, found that 98% of companies surveyed out of 200 had suffered a cloud data breach “in the past 18 months compared to 79% last year.”). Out of the companies who experienced a breach in their cloud security “63% said they had sensitive data exposed.” See also Why is Corporate Cybersecurity Important?, RECIPROCITY (Feb. 10, 2022), archived at https://perma.cc/LX88-HXKN (highlighting the importance of cybersecurity practices as cyber hackers employ more complicated techniques). Data breaches are becoming more sophisticated as cyberattacks become more advanced, the availability of hacking tools is increasing, and the proliferation of devices connected to the internet continues to grow. See also IBM Report, supra note 7 (discussing how 60% of organizations have moved into cloud-based activities during the pandemic). The issue with cloud-based activities is that security is lagging “behind these rapid IT changes, hindering organizations’ ability to respond to data breaches.” See also IBM Report, supra note 7.
B. The Beginning of the Chief Information Security Officer

In order to solidify internal security within companies, the role of Chief Information Security Officer (CISO) is a position that emerged in 1995 when Citicorp, now Citigroup, hired Steve Katz, the first ever CISO.\(^{32}\) Katz was originally appointed to be CISO of Citicorp to augment digital defenses from cyberhackers in Russia.\(^{33}\) The initial responsibilities of CISOs following Katz were mainly technical in nature requiring only some infrastructure and IT expertise.\(^{34}\) However, this role has continuously expanded, and now CISO responsibilities include maintaining the knowledge of cloud computing, mobile devices, and new technological advancements as cyberattacks escalate.\(^{35}\) This ongoing cyber development makes the role for CISOs working at major corporations an increasingly difficult job with the intensifying pressure of maintaining sizable defense

\(^{32}\) See Evolution of the Chief Information Security Officer, INST. WORLD POL. (Oct. 19, 2022), archived at https://perma.cc/P2DH-KGCQ (highlighting how Katz was the first CISO to be appointed). “The CISO role was designed as a response to the ever-increasing need to maintain the security of information and operations contained within the internal technology infrastructures upon which operations relied.” Id.

\(^{33}\) See Steve Morgan, Backstory Of The World’s First Chief Information Security Officer, CYBERCRIME MAG. (Oct. 13, 2020), archived at https://perma.cc/5HXU-G4Y3 (reviewing how the CISO position was first created by Citicorp and Steve Katz was appointed to the role). During the 1990s, it was thought that this position was not necessary due to the “size, complexity and scale” of technology being much less complicated than what CISOs are handling now. Id. See also Amy Harmon, Hacking Theft of $10 Million From Citibank Revealed, L.A. TIMES (Aug. 19, 1995), archived at https://perma.cc/N9DD-RM33 (describing how Russian nationals hacked a former Citigroup computer system in 1995 and stole more than $10 million through wiring the money into various global accounts).

\(^{34}\) See Nick Puetz & Farid Abdelkader, C-Suite Shuffle: The CISO’s Evolving Role and Reporting Structure, CSO (Mar. 15, 2022), archived at https://perma.cc/2JDVF-7U8 (discussing the original role of CISOs).

\(^{35}\) See Morgan, supra note 33 (discussing how cloud computing and mobile devices have augmented the complexities of technology and intensified cyber activities being carried out by hostile cyberattacks and countries). See also IBM Report, supra note 7 (stressing that the shift to the cloud has increased the severity and number of data breaches). “Companies in the study that experienced a breach during a cloud migration project had 18.8% higher cost than average.” Id. However, having a hybrid-cloud environment actually decreased the average cost of a data breach. Id. See also Damouni, supra note 23 (discussing how the CISO role is evolving to be viewed more as a business risk than a compliance issue).
systems for involute cybersecurity difficulties. CISOs also now sustain many diverse roles on top of cyber defense advocacy such as maintaining relationships, providing leadership for security challenges, and upholding the company’s cybersecurity program. In addition to the surging complexity of cybersecurity, CISOs moreover must combat goal-centered executives within their corporations who do not always view bolstering security as a top priority.

CISOs are on the C suite and report to different executives, such as the Chief Information Officer (CIO), Chief Financial Officer (CFO), or Chief Executive Officer (CEO) to ensure cybersecurity compliance within the entirety of the company. There has recently been a shift away from CISOs reporting to the CIO as companies slowly expand the idea that cybersecurity is a company-wide issue, not

---

36 See CISOs Have the Toughest Job in the World, BALBIX (Oct. 24, 2022), archived at https://perma.cc/LW46-HLN8 (pointing out the high stakes a CISO has to manage daily). “Today’s CISOs face daunting challenges. They are constantly fending off increasingly sophisticated attacks, balancing scarce resources, and working with a board that too often doesn’t understand the inevitability of a breach and the criticality of the CISO’s role.” Id.

37 See Curtis Simpson, The Evolving Role of the CISO, THREATPOST (July 16, 2021), archived at https://perma.cc/23NR-8AT9 (noting the importance of the CISO position and top qualities a CISO must have including being a relationship builder, leader, and advocate).

38 See Sabin, supra note 14 (discussing how CISOs and CEOs are required to get the “buy-in of their chief executive officers and boards to get the staffing and budget they need to properly secure their operations.”). Requiring a CISO to get the approval of top executives poses issues to their security infrastructure if executives are in disagreement with their defense mechanisms. Id.

39 See Poremba, supra note 9 (pointing out that CISOs can work with CEOs or CIOs). The only way the CISO can do their job is to have the full support of the CEO. Therefore, CEOs can no longer afford to ignore their digital defenses. It’s up to the CEO to make sure the CISO and the security team have the budget and resources – including the right tech and staffing – necessary to meet today’s challenges. It is also up to the CEO to make sure the CISO has the authority necessary to make decisions.

Id. See Mishra, supra note 12 (describing how CISOs report cases to the executive board). Since CISOs don’t have control of their budget they don’t have executive authority to make decisions therefore they are not typically held liable for data breaches. Id.
just an IT issue. Therefore, reporting to the CEO is becoming more commonplace as it is thought to increase coordination of cybersecurity goals within the company. On top of reporting duties, CISOs also have a responsibility to maintain relationships with the employees within the company so that cybersecurity is properly acknowledged and respected by the company as a whole. Therefore, due to the multifaceted nature of the responsibilities of this role, it can be an extremely challenging one to balance.

C. Background on the Federal Trade Commission

The Federal Trade Commission (FTC), otherwise known as the Commission, is the federal agency who has headed investigations on data breaches since 1970. The goal of the FTC is to protect American’s privacy and identify the areas of priority to appropriately

40 See Evolution of the Chief Information Security Officer, supra note 32 (pointing out that CISOs can report to the CEO or CIO within the corporation depending on the specific companies’ requirements). See Puetz & Abdelkader, supra note 34 (describing the move away from CISOs reporting to the CIO). Reporting to the CEO has benefits such as aligning corporate oversite, strengthening the role when the CIO accepts too much risk, and reducing the idea that cybersecurity is only an IT issue. Id. However, if a CISO reports to the CIO, then their authority within IT and reducing the CISO team’s workload due to coordination with IT. Id. 41 See Puetz & Abdelkader, supra note 34 (furthering the idea that reporting to a CEO increases the CISOs authority outside of IT work). See also Sabin, supra note 14 (pointing out that CISOs usually report to their CEOs or the board of directors). However, many CISOs “struggle to see eye to eye with their organizations’ CEOs or company boards” which is problematic to ensuring they are properly maintaining their security role in the company. Id. 42 See Ajay Unni, 10 Key Roles a CISO Plays in an Organization, STICKMANCYBER (Oct. 19, 2022), archived at https://perma.cc/4HH7-L8B8 (listing the numerous important roles that a modern CISO must fulfill). 43 See Susan Caminiti, Chief information security officers say stress and burnout, not job loss as a result of a breach, are their top personal risks, CNBC (Sept. 8, 2022), archived at https://perma.cc/5CUW-FP57 (detailing personal accounts from various CISOs regarding the immense stress they face due to the continuous expansion of technology). A CISO, Daniel Combs, notes that “breaches and the tech talent shortage are contributing to the mounting stress and burnout that CISOs are experiencing.” Id. Combs points out how it is incredibly important CISOs have support from every member of a company including “the executive team and board, including financial investments.” Id. 44 See Protecting Consumer Privacy and Security, FTC (Oct. 18, 2022), archived at https://perma.cc/XD5T-3HAA (declaring how the FTC is the “chief federal agency on privacy policy and enforcement” since the start of security breaches).
shield them. The FTC’s scope of legal authority is found in multiple places, including, Section 5 of the FTC Act which bans deceptive or unfair commercial acts, as well as within a variety of specified laws in the privacy field. The three prong unfairness test used by the FTC states that an act by a company is considered unfair if it is likely to cause substantial injury to consumers, is not reasonably avoidable by consumers, or is not outweighed by benefits to consumers or competition. An act is considered deceptive when there is a material representation by a company that is likely to mislead a consumer. If there is no deceptive misrepresentation or the act does not fit into the three prong unfairness test, the FTC does not have legal authority to pursue a claim against a company. However, even if the Commission does not pursue a claim against a company, individual offices of the U.S. Department of Justice may still file claims against companies and individuals for data breaches.

45 See FTC REP. TO CONG. ON PRIV. AND SEC., 1, 3 (2021) (describing the four areas of priority that the FTC is working to improve the effectiveness of in order to defend American’s privacy). The FTC has “four areas of FTC focus for improving the effectiveness of [their] efforts to protect Americans’ privacy: integrating competition concerns, advancing remedies, focusing on digital platforms, and expanding on [their] guidance on and understanding of the consumer protection and competition implications of algorithms.” Id.

46 See 15 U.S.C. § 45 (2011) (declaring that the FTC has the power to prevent any persons or corporations from using unfair or deceptive acts or practices). See also FTC REP. TO CONG. ON PRIV. AND SEC., supra note 45, at 2 (noting where the FTC receives its authority to act). The FTC has the power to enforce specific laws, some including the Gramm-Leach-Bliley act, which protects the privacy of financial information; the CAN-SPAM Act, permitting consumers to refuse commercial emails; and the Fair Credit Reporting Act, which protects privacy of consumer report information. Id.

47 See 15 U.S.C. § 45(n) (2011) (describing what constitutes unfair or deceptive acts). The FTC only has authority to declare an act or practice unlawful if it meets these qualifications. Id.

48 See FTC POLICY STATEMENT ON DECEPTION, 103 F.T.C. 110, 174 (1984) (explaining what practices must exist for deception to be present in a company). Some examples of “[p]ractices that have been found misleading or deceptive in specific cases include false oral or written representations[.]” Id.

49 See FTC REP. TO CONG. ON PRIV. AND SEC., supra note 45, at 1 (summarizing when the FTC can legally pursue a company).

50 See U.S. Dep’t of Just., Just. Manual § 0900.00.01 (2018) (detailing the DOJ’s procedures for actual or suspected data breaches). See also FTC REP. TO CONG. ON PRIV. AND SEC., supra note 45, at 6–7 (noting how the Department of Justice can file
As such, the Commission enforced one of the first federal privacy laws, the Fair Crediting Reporting Act, which protects the privacy of consumer information contained in files from consumer reporting agencies.\(^1\) Since then, the FTC has pursued 80 data security reviews from 2002 to 2021 of corporations involved in major data breaches where poor cybersecurity mechanisms were possibly implemented.\(^2\) The Commission historically seeks relief for customers by punishing the company and its practices as a whole rather than pursuing any individual or groups of corporate executives within the company.\(^3\) The FTC customarily seeks injunctive relief from companies who are found to have violated the Federal Trade Commission Act (FTA).\(^4\) Since their creation, the FTC is only increasing regulatory charges, by augmenting governmental enforcement of data security standards.\(^5\)

---


\(^2\) See FTC REP. TO CONG. ON PRIV. AND SEC., supra note 45, at 3 (citing the number of cases the FTC has brought against companies who have undertaken “unfair or deceptive practices involving inadequate protection of consumers’ personal data.”).

\(^3\) See id. at 4 (describing who the FTC legally pursues for claims of data and security breaches). See e.g., Ashley Madison v. Ruby Corp, Ruby Life Inc., 152 F.T.C. 3284, 1, 15 (2017) (providing an example of how the FTC typically punishes a company and not an executive).

\(^4\) See 15 U.S.C. §§ 41–58 (2006) (noting the FTC’s primary statute of the Commission). The Federal Trade Commission Act allows the FTC to seek monetary, injunctive, or other methods of relief for acts which injure customers. Id. See also FTC REP. TO CONG. ON PRIV. AND SEC., supra note 45, at 1–2 (describing forms of injunctive relief including the implementation of privacy and data security programs, deleting data developed with user data, and consumer consent). See also DSW Inc. Settles FTC Charges, supra note 21 (describing an example of the FTC seeking injunctive relief with a company who violated the FTC Act). The settlement with DSW required the company “to implement a comprehensive information-security program and obtain audits by an independent third-party security professional every other year for 20 years.” Id.

\(^5\) See Brenda R. Sharton & Gerard M. Stegmaier, Breaches in the boardroom: What directors and officers can do to reduce the risk of personal liability for data security breaches, REUTERS (Sept. 21, 2022), archived at https://perma.cc/J5SU-K5M9 (pointing out how the FTC states that the number of regulatory charges is only “likely to go up” in the future).
D. The Federal Trade Commission’s Response to Data Breaches

The FTC is the main federal office where companies are required to report data breaches and cyber issues to the government. The FTC recently expanded their standards pursuant to Section 5 of the FTC Act to include a company’s failure to notify the Commission of a data breach in an adequate time period as a breach of the Act. The FTC established this heightened standard through a multitude of precedent cases with companies such as CafePress, SpyFone, and SkyMed. The Commission found that CafePress failed to notify

56 See Security Beyond Prevention: The Importance of Effective Breach Disclosures, FTC (May 20, 2022), archived at https://perma.cc/Y3PE-X9H8 (exemplifying when and why data breaches should be reported to the FTC in a timely manner). “Regardless of whether a breach notification law applies, a breached entity that fails to disclose information to help parties mitigate reasonably foreseeable harm may violate Section 5 of the FTC Act.” Id. “[C]ompanies have legal obligations with respect to disclosing breaches, and these disclosures should be accurate and timely. Effective detection and response capabilities are core components of a security program and when they fail, companies should effectively and completely disclose what happened.” Id.

57 See Anna Rudawski & Chris Cwalina, FTC Signals Additional Scrutiny for Data Breaches, NORTON ROSE FULBRIGHT LLP (May 25, 2022), archived at https://perma.cc/D6QZ-JLKM (discussing how the FTC recently updated what constitutes a violation of Section 5 of the FTC act). If a company does not disclose a data breach to the FTC in a timely manner, then they may be in violation of Section 5 of the FTC Act. Id. See also Security Beyond Prevention: The Importance of Effective Breach Disclosures, supra note 56 (explaining the FTC’s position and decision to expand breach disclosure for companies). “When security breaches do occur, timely, accurate, and actionable security disclosures can, when done well, fulfill legal obligations and be essential to enabling consumers and other affected parties to take actions to mitigate harm resulting from the breach.” Id.

58 See Security Beyond Prevention: The Importance of Effective Breach Disclosures, supra note 56 (discussing the deceptive actions that CafePress, SpyFone, and Skymed took to conceal data breaches).

Taken together, these cases stand for the proposition that companies have legal obligations with respect to disclosing breaches, and that these disclosures should be accurate and timely. Effective detection and response capabilities are core components of a security program and when they fail, companies should effectively and completely disclose what happened.

Id. See e.g. In the Matter of CafePress, C-4768 LLC F.T.C. 1923209, 21 (2022) (discussing the case against CafePress regarding a data breach). The FTC sought
customers and relevant parties that data breaches had occurred for months preventing them from protecting their personal information. Since CafePress did not disclose the data breach to customers and the FTC in a timely manner, the Commission heavily considered this failure of notification in its stringent orders against CafePress. While SkyMed similarly deceived customers and the FTC by making erroneous public statements about data breaches which were affecting their company, resulting in the FTC ordering an augmentation of security measures and transparency from SkyMed. The case of SkyMed demonstrated that companies can be pursued for a failure to promptly disclose data breaches regardless of whether the company is

relief for customers when CafePress committed unfair data security practices and covered up multiple data breaches. See In the Matter of SkyMed Int’l, Inc., C-4732 F.T.C. 1923140, 3 (2021) (pointing out how the FTC pursued SkyMed for not reporting a data breach within an adequate time period). See also In the Matter of Support King, LLC, C-4756 F.T.C. 192 3003, 10 (2021) (highlighting how SpyFone, now Support King, did not report a data breach in a timely manner). See also FTC Takes Action Against CafePress for Data Breach Cover Up, FTC (Mar. 15, 2022), archived at https://perma.cc/73JJ-NS3H (describing how CafePress knew of their security vulnerability and data breach but did not inform affected customers and the FTC for six months after the breaches were first reported). CafePress did not inform consumers of the breach in a timely manner and “allow[ed] people to reset their passwords on the website by answering security questions associated with customer email addresses—the same information that had been previously stolen by hackers.” Id. at 3, 10–12. See also Lesley Fair, Data breach prevention and response: Lessons from the CafePress case, FTC (Mar. 15, 2022), archived at https://perma.cc/D9Q6-4AAW (detailing what companies should take away from CafePress’s data security failure). CafePress is ordered to pay “$500,000 in redress and to send notices to consumers telling them about the breach and the FTC settlement.” Id.

See In the Matter of CafePress, C-4768 LLC F.T.C. 1923209, 21 (2022) (finding that CafePress violated the Federal Trade Commission Act). See also FTC Takes Action Against CafePress for Data Breach Cover Up, FTC (Mar. 15, 2022), archived at https://perma.cc/73JJ-NS3H (describing how CafePress knew of their security vulnerability and data breach but did not inform affected customers and the FTC for six months after the breaches were first reported). CafePress did not inform consumers of the breach in a timely manner and “allow[ed] people to reset their passwords on the website by answering security questions associated with customer email addresses—the same information that had been previously stolen by hackers.” Id. at 3, 10–12. See also Lesley Fair, Data breach prevention and response: Lessons from the CafePress case, FTC (Mar. 15, 2022), archived at https://perma.cc/D9Q6-4AAW (detailing what companies should take away from CafePress’s data security failure). CafePress is ordered to pay “$500,000 in redress and to send notices to consumers telling them about the breach and the FTC settlement.” Id.

See In the Matter of SkyMed Int’l, Inc., C-4732 F.T.C. 1923140, 5–6, 9 (2021) (ordering SkyMed to implement increased security measures and make timely submissions to the FTC to ensure the company has proper security protocols). See also Security Beyond Prevention: The Importance of Effective Breach Disclosures, supra note 56 (pointing out that “deceptive statements can hinder consumers from taking critical actions to mitigate foreseeable harms like identify theft, loss of sensitive data, or financial impacts.”). These negative repercussions elucidate why the FTC recently began to take into account failure for timely and accurate information disclosing data breaches. Id.
in a breach notification state or if federal law applies. This standard expansion is significant because historically company leaders have been resistant to immediately sharing knowledge of data breaches within their companies until they understand the full repercussions of the transgression, leading to increased harm to affected consumers.

E. Companies Coverup of Data Breaches and Blame Placed on the CISO

Many companies, especially those on the Fortune 500 list, have traditionally concealed data breaches to avoid public backlash and federal or civil proceedings against them. Though there is no exact data statistic, it is estimated that well over 20% of companies have hidden or suppressed a breach according to a survey of security professionals working at a variety of larger companies. Due to the information used for this estimation, this number is likely grossly underestimated- but it regardless provides insight into the commonality of breaches which are suppressed from public and

62 See Bhuiyan, supra note 16 (discussing common state data breach standards). Most U.S. states have regulations mandating how public disclosures must be made “in the most expedient time possible and without unreasonable delay.” Id. See also Mark Rasch, Privacy as Property: Uber CISO Criminal Case Goes to Trial, SEC. BOULEVARD (Sept. 14, 2022), archived at https://perma.cc/8FEZ-XSGF (pointing out that “data breach disclosure laws do not have criminal penalties” and they only allow companies to be fined for violations). See Security Beyond Prevention: The Importance of Effective Breach Disclosures, supra note 56 (discussing how even if a breach notification law does not apply, “a breached entity that fails to disclose information to help parties mitigate reasonably foreseeable harm may violate Section 5 of the FTC Act.”).

63 See id. (pointing out the multitude of companies who have avoided disclosing breaches to the FTC).

64 See Report: 1/4 of Fortune 500 Companies Hacked in Last Decade, VPNMENTOR (Oct. 24, 2022), archived at https://perma.cc/M9WU-53UK (discussing how Fortune 500 companies actually experience more cyberattacks than smaller companies). The larger the company is on the Fortune 500 list, the higher data breaches that company experienced. Id.

65 See 20% of security professionals say their company has hidden or covered up a breach, IT GOVERNANCE (May 18, 2015), archived at https://perma.cc/LJF9-E646 (pointing out how in a recent survey by AlienVault with over 1000 people, they found twenty percent of respondents observed a company hide a breach).
This precedent of concealment is problematic as it is now catching up to companies and their illegal practices.67

The customary standard of concealment proves complicated for executives such as CISOs.68 When concealment is exposed or revealed, and data breaches come to light, CISOs have often been held responsible for the cyber failure.69 It is common that CISOs are used as a scapegoat for cybersecurity hacks and problematic cyber incidents.70 As a result, many CISOs are fired or publicly blamed for these controversial cyber affairs, however, no CISO had ever been held

66 See e.g. Ashley Belanger, T-Mobile to pay $500M for one of the largest data breaches in US history, ARS TECHNICA (July 25, 2022), archived at https://perma.cc/WBJ4-DZ5J (discussing the T-Mobile breach and how T-Mobile is now in a class action lawsuit for continuing to profit off data while covering up a massive data breach). T-Mobile is an example of a common practice major corporations take; covering up data breaches by not disclosing information to the public or the FTC to avoid repercussions. Id.

67 See Robert McMillan, Trial of Former Uber Executive Has Security Officials Worried About Liability for Hacks, WALL. ST. J. (Sept. 8, 2022), archived at https://perma.cc/D7UW-Q24X (noting how “it is common for companies to keep quiet about some security incidents, especially if the evidence that data was misused is hard to find.”).

68 See Lily Hay Newman, The Uber Data Breach Conviction Shows Security Execs What Not to Do, WIRED (Oct. 7, 2022), archived at https://perma.cc/PPF4-TDLM (highlighting how CISOs are sometimes referred to as “chief sacrificial officers” because of how challenging securing a massive corporation can be).

69 See Ben Kochman, Yes, You Can Face Prison Time For Hiding A Data Breach, LAW360 (Oct. 6, 2022), archived at https://perma.cc/QU4K-EY3B (discussing how it should not be a surprise that many CISOs coverup data breaches due to mounting pressures of the job). See also CISOs Have the Toughest Job in the World, supra note 36 (highlighting that “[w]hen a company suffers a breach, everyone looks to the CISO for answers.”). CISOs are mainly recognized for their failures when data breaches occur rather than their successes such as prevented attacks. Id.

70 See Former Uber CISO Convicted: What, How, & Why?, CYBER MGMT. ALL. (Oct. 11, 2022), archived at https://perma.cc/Q9RH-D6YX (discussing how CISOs have historically been “scapegoat[s] for security incidents.”). See also Hill & Browning, supra note 14 (noting that CISOs do not “generally make the call on whether a company reports a data breach.”). See also Kochman, supra note 69 (pointing out how when data breaches occur, they are extremely overwhelming for security professionals). “When a company is under a cyberattack, the pressure and demands upon tech personnel can become overwhelming, and it can be tempting to try to cover up what could be perceived as mistakes[.]” Id. See John Armstrong, The Role of the CISO in Preventing Data Breaches, FORTRA (Feb. 20, 2018), archived at https://perma.cc/M7EA-S9FC (pointing out that “21 percent of IT decision-makers would most likely blame a data breach on the CISO”).
criminal liability for a company’s data breach until Joseph Sullivan. The custom of concealment and blame placement on CISOs has created an increasingly stressful culture for CISOs to work in, which is why some CISOs do aid in covering up breaches within their company to avoid being condemned for a data breach or being fired.

III. Facts

A. The FTC’s Investigation in the 2014 and 2016 Uber Data Breaches

_U.S. v. Sullivan_ is an instrumental case in the cybertechnology sphere as it is the first time a CISO has been criminally convicted for a data breach leaving many split on this conviction. Joseph

---

71 See Hill & Browning, supra note 14 (pointing out that CISOs have never been prosecuted and convicted of a cover up of a data breach). See also The Hacked & the Hacker-for-Hire: Lessons from the Yahoo Data Breaches (So Far), BALLARD SPAHR (May 11, 2018), archived at https://perma.cc/6YD6-LBMJ (describing when the CISO of Yahoo discovered the security breach, he told Yahoo’s senior management within days). See also Stephen Boyer, We’re all at risk when 65% of stressed-out cybersecurity and IT workers are thinking about quitting, tech exec warns, CNBC (Oct. 11, 2019), archived at https://perma.cc/C8DK-LASS (citing “the average tenure of a chief information security officer (CISO) is only 18 to 24 months” due to heightened pressure and turnover rates). See also Sabin, supra note 14 (highlighting how CISOs are used to being used to being scapegoated). “CISOs are used to being either fired or publicly blamed for a company security incident.” Id.

72 See Hill & Browning, supra note 14 (explaining how CISOs have an increasingly tricky job “ensuring that their companies’ data remains safe from hackers and fraudsters . . .”). CISOs have a “high-stakes job” as they are held responsible for data breaches. _Id._ See also Joseph Menn, Former Uber security chief convicted of covering up 2016 data breach, WASH. POST (Oct. 5, 2022), archived at https://perma.cc/5E3B-W9EC (discussing how it is common for companies to use bug bounty programs to cover up data breaches and pay off hackers). “Casey Ellis, founder of Bugcrowd, acknowledged that some companies use bounty programs to hush up problems that should have been disclosed under state or federal rules.” _Id._ Since the amount of data security attacks have greatly increased since Sullivan was fired from Uber five years ago this type of nondisclosure and dealing with hackers has only increased. _Id._ It is now seen as “routine” for companies to payoff extortionists almost as “similar to a fender bender” according to Michael Hamilton, a founder of a security firm. _Id._

73 See Menn, supra note 72 (describing how Sullivan’s conviction came as a shock to many who were expecting his acquittal). This case is so important as it potentially
Sullivan’s case began in May of 2015, when the FTC served a Civil Investigative Demand on Uber seeking information about Uber’s data security program, practices, and instances of unauthorized access to user personal information following a cyber incident which arose in 2014 at Uber.\textsuperscript{74} Joseph Sullivan, Uber’s security executive at the time, was incredibly involved within this investigation and on November 4, 2016, testified under oath that Uber had taken significant steps to protect consumer data through increased security practices.\textsuperscript{75} However, ten days later Sullivan and other Uber executives received an email, which was quickly verified, from anonymous hackers creates a precedent where CISOs may be held criminally liable for data breaches which may not be solely their fault. \textit{Id.}

\textsuperscript{74} See Dr. Nick Oberheiden, \textit{Seven Critical Steps to Follow if You Receive a Civil Investigative Demand}, 12 NAT’L L. REV. (Mar. 25, 2021) (defining Civil Investigative Demands as “powerful investigative tools that the U.S. Department of Justice (DOJ) and other federal agencies use to gather evidence in support of civil charges.”). \textit{See also} 18 U.S.C. § 1968 (1970) (noting the statute for a Civil Investigative Demand).

Whenever the Attorney General has reason to believe that any person or enterprise may be in possession, custody, or control of any documentary materials relevant to a racketeering investigation, he may, . . . issue in writing, and cause to be served upon such person, a civil investigative demand requiring such person to produce such material for examination. \textit{Id.} \textit{See also} Press Release, U.S. Att’y’s Off. N.D. Cal., Former Chief Security Officer Of Uber Convicted Of Federal Charges For Covering Up Data Breach Involving Millions Of Uber User Records (Oct. 5, 2022) (on file with author) \textit{[hereinafter Former Chief Security Officer Of Uber Convicted]} (discussing how the Civil Investigative Demand on Uber required thorough details about all instances of “unauthorized access to user personal information, and information regarding Uber’s broader data security program and practices.”). The Civil Investigative Demand was a result of Uber’s disclosed data breach in 2014 which resulted in “50,000 consumers’ personal information” leaked. \textit{Id.}

\textsuperscript{75} See Former Chief Security Officer Of Uber Convicted, \textit{supra} note 74 (detailing the timeline of the original FTC investigation of Uber in 2016 and Joseph Sullivan’s involvement). Pointed out that Joseph Sullivan’s testimony encompasses “specific representations about steps he claimed Uber had taken to keep customer data secure.” \textit{Id.} \textit{See also} Press Release, U.S. Att’y’s Off. N.D. Cal., Former Chief Security Officer for Uber Charged With Obstruction of Justice (Aug. 20, 2020) (highlighting how Sullivan discussed questions and security protocols with the FTC during the investigation for the 2014 hack under oath). \textit{See also} Matthew Yarbrough, \textit{An Uber to Prison: Lessons Learned from a Convicted CSO}, MICHELMAN & ROBINSON (Oct. 20, 2022), archived at https://perma.cc/M7LP-EHUT (elaborating on what specifically Sullivan discussed with the FTC). “Sullivan had outlined to the FTC the steps Uber had taken to fix and improve the company’s security program in the wake of the 2014 incident, going so far as to claim that measures were put in place to prevent any additional breaches that targeted the same vulnerabilities.” \textit{Id.}
detailing a new data breach and demanding a ransom payment for the information to be deleted. The hackers obtained access to personally identifiable information comprised of 57 million riders and drivers including 600,000 Uber drivers’ license numbers. Despite being under investigation for a previous data breach, Sullivan did not inform the FTC of this new breach and decided to tightly control this situation by offering to pay the hackers $100,000 in bitcoin in exchange for signed non-disclosure agreements promising that they would not discuss the breach with anyone. The hackers agreed to sign the non-
disclosure forms, which falsely stated that they had not taken or stored any data during the breach.\textsuperscript{79} Sullivan then paid the hackers through the company’s bug bounty program without reporting it to the FTC during their inquiry or to the General Counsel of Uber, but did inform and receive approval for his actions from the then CEO and co-founder of Uber, Travis Kalanick.\textsuperscript{80} 

Joseph Sullivan immediately informed Kalanick of the data breach and, following the advice of both Kalanick and one of Uber’s in-house security lawyers, Craig Clark, decided that it was not necessary to report the 2016 breach to the FTC.\textsuperscript{81} However, when

\textit{See also} Lakshmanan, \textit{supra} note 76 (describing how Uber secretly paid a ransom payment of \$100,000 and required the extortionists to sign a non-disclosure agreement).\textsuperscript{79} \textit{See Sullivan}, 2022 U.S. Dist. LEXIS 154594, at *5 (pointing out that Sullivan made a misrepresentation regarding the non-disclosure agreement when he “stat[ed] [that] the hackers did not take or store Uber’s data[,]”). \textit{See also Yarbrough, supra} note 75 (discussing in detail the misrepresentation that Sullivan made regarding the non-disclosure agreement). “[T]he hackers were required to sign a nondisclosure agreement drafted by Sullivan and Uber’s in-house lawyer that included a false ‘promise’ and a statement that the hackers ‘did not take or store any data during or through [their] research.’” \textit{Id.}  

\textit{See What are Bug Bounties? How Do they Work? [With Examples], HACKERONE} (July 16, 2021), \textit{archived at} https://perma.cc/4JNA-RTYF (describing how bug bounty programs are utilized in public and private companies). A company who has a bug bounty program has a budget and scope for what systems hackers can test and the amount of money ethical hackers will receive if they find a vulnerability in the cybersecurity system. \textit{Id.} \textit{See also} Lakshmanan, \textit{supra} note 76 (pointing out that Kalanick approved of “Sullivan’s strategy for handling the unauthorized intrusion[,]” but never testified and has yet to be charged). Sullivan secretly transferred money to the unethical hackers in an effort to attribute the hack to a bug bounty program – a program where ethical hackers are paid for the purpose of identifying vulnerabilities. \textit{Id.} \textit{See also} Mike Isaac et al., \textit{Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data}, N.Y. TIMES (Nov. 21, 2017), \textit{archived at} https://perma.cc/D5H2-SY2L (describing how Kalanick arranged the deal with the cyberhackers). \textsuperscript{80}  

\textit{See Rob Chesnut, Uber Security Chief’s Conviction Raises Red Flags: Good Counsel, BLOOMBERG L.} (Oct. 12, 2022), \textit{archived at} https://perma.cc/DT2F-3BVF (pointing out that Sullivan discussed the breach with CEO, Travis Kalanick and specifically followed the advice of Uber’s lawyer, Craig Clark). Joseph Sullivan did not report the data breach to the federal government after being advised by Uber’s in-house privacy lawyer that it was not necessary. \textit{Id.} Craig Clark was an in-house lawyer at Uber and a member of the security group which handled the breach. \textit{Id.} \textit{See Maria Dinzeo, Former Uber general counsel testifies ex-security chief downplayed 2016 data breach, COURTHOUSE NEWS SERV.} (Sept. 15, 2022), \textit{archived at} https://perma.cc/8YK5-8CMR (explaining how it is still “murky” regarding how much the C-suite of Uber knew about the 2016 data breach). Sullivan told the
Kalanick was forced to step down for separate reasons, Uber’s new management began investigating facts surrounding the 2016 breach. As a result, Sullivan eventually informed the new CEO of Uber, Dara Khosrowshahi, of the full scope of the 2016 data breach, which resulted in Khosrowshahi firing Sullivan and other Uber employees who were involved in handling the breach. Unfortunately, Kalanick and Clark’s original advice to not disclose this incident proved to be a massive mistake leading to broad implications surrounding the security world regarding CISOs and regulations.

security response team and Clark that he was in direct communications with Kalanick and other members of the “A-team[,]” however, top members of Uber, such as the general counsel, vehemently denies knowing details of the breach. Id. See Kate Conger, Uber Founder Travis Kalanick Leaves Board, Severing Last Tie, N.Y. TIMES (Dec. 24, 2019), archived at https://perma.cc/XH95-KPVR (discussing that Kalanick was forced to step down as CEO of Uber “after a series of privacy scandals and complaints of discrimination and sexual harassment at the company.”). Dara Khosrowshahi, former executive at Expedia, took the place of Travis Kalanick when he resigned as CEO. Id. See Cade Metz, Uber Boss Testifies He ‘Could Not Trust’ Ex-Security Chief,’ N.Y. TIMES (Sept. 16, 2022), archived at https://perma.cc/Z2E3-89ZV (detailing how when Khosrowshahi became CEO, he begun an investigation into the 2016 data breach). Khosrowshahi asked Sullivan about details regarding the breach and in his response, Sullivan did not disclose that “hackers had downloaded personal information about drivers and riders” and that Sullivan had paid them off with a six figure ransom. Id.

See Menn, supra note 72 (depicting how Sullivan initially portrayed the 2016 data breach as a “routine payoff” and edited the details of the amount of payoff and information the hackers obtained). “After a later investigation turned up the full story, Khosrowshahi testified, he fired Sullivan for not telling him more sooner.” Id. See also Richard Lawler, Former Uber security chief found guilty of covering up massive 2016 data breach, VERGE (Oct. 5, 2022), archived at https://perma.cc/XUF9-RRTX (discussing how Sullivan was fired by Khosrowshahi, the new CEO of Uber, after finding out about the complete details of the 2016 data breach). See also Dinzeo, supra note 81 (explaining how Sullivan sent a “three-paragraph summary of what had transpired” to General Counsel Salle Yoo and CEO Dara Khosrowshahi in September 2017).

See Chesnut, supra note 81 (explaining how Kalanick and Clark’s advice to Sullivan of not reporting the data breach of 2016 to the FTC was a great mistake for not only Sullivan, but others such as lawyers within the field). Sullivan’s “conviction highlights the very real personal consequences facing corporate executives if hacks are not properly handled.” Id. “[A] cloud hangs over the profession and may lead some of the best and brightest in the [cybersecurity] field to think twice before taking a top in-house security job.” Id.
B. Details of United States v. Sullivan

In 2020, Joseph Sullivan was the only individual charged with obstructing a federal proceeding, misprision of felony, and wire fraud counts due to his alleged cover up of the Uber data breach and scheme to defraud Uber drivers. At the time of Sullivan’s “cover up,” there was no statute mandating companies to disclose data security breaches to the federal government, therefore, the Department of Justice (DOJ) used these three broad charges to prosecute Sullivan. The DOJ took

85 See 18 U.S.C. § 1505 (noting the statute for Obstruction of Justice). “Whoever, with intent to avoid, evade, prevent, or obstruct compliance in whole or in part, with any civil investigative demand duly and properly made under the Antitrust Civil Process Act, willfully withholds, misrepresents, removes from any place, conceals, covers up, destroys . . . any evidence relating to that demand, violates this statute. Id. A person found guilty may be “fined under this title [or] imprisoned not more than 5 years . . . or both.” Id. See also 18 U.S.C. § 4 (noting the statute for misprision of a felony). A person is liable under 18 U.S.C. § 4 if they have knowledge of the “actual commission of a felony” and conceals this knowledge. Id. If found guilty a person “shall be fined under this title or imprisoned not more than three years, or both.” Id. See 18 U.S.C. § 1343 (noting the statute for fraud by wire).

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both.

Id. See Sullivan, No. 20-CR-00337-WHO-1, 2022 WL 2317441, at *1 (describing the charges in which Sullivan was charged with). Sullivan is the only Uber employee to be charged for the 2016 data breach. Id.

86 See Kellen Dwyer et al., Uber Exec Trial Is A Lesson In Handling Data Breach Incidents, LAW360 (Oct. 25, 2022), archived at https://perma.cc/9WAP-ZR9X (describing how there is no statute which mandates “companies to disclose data security incidents to the federal government.”). However, there is a statute that will likely take effect in 2025 that President Biden “recently signed legislation [which] require[es] companies considered critical infrastructure to report data security incidents in certain circumstances.” Id. See also CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022 (CIRCIA), CISA (Nov. 14, 2022), archived at https://perma.cc/3B76-T2W2 (describing the CIRCIA Act President Biden signed in March 2022). This new statute allows “the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments . . . .” Id. CIRCIA will require companies that experience data breaches to report them within a 72-hour period. Id. See also Michael T. Borgia, The Cyber Incident Reporting for Critical Infrastructure Act of 2022: An Overview, DAVIS
the position that Sullivan had obstructed the FTC’s investigation because the FTC assumed that he was required to continuously update the Civil Investigative Demand for the previous 2014 breach, and Sullivan failed to do so. The government argued that a company is required to update statements and testimony regarding new incidents’ that take place when a government investigation is occurring, including an FTC investigation. The DOJ supported the charge of misprision of felony by interpreting the actions taken by Sullivan, specifically his misuse of the Uber’s bug bounty program to pay the hackers for their silence, as a showing of his awareness that a felony

WRIGHT TREMAINE LLP (May 18, 2022), archived at https://perma.cc/8D48-NZ73 (pointing out how CIRClA will be an effective rule to counter cyberattacks and ransomware issues). See also Security Beyond Prevention: The Importance of Effective Breach Disclosures, supra note 57 (describing how the FTC enforces timely and accurate security disclosures through precedent case law). See also Dr. Keri Pearlson & Chris Hetner, Is Your Board Prepared for New Cybersecurity Regulations?, HARV. BUS. R. (Nov. 11, 2022), archived at https://perma.cc/4JHH-K6L9 (discussing the newly proposed rule from the SEC).

87 See Former Chief Security Officer Of Uber Convicted, supra note 74 (discussing how technology companies are expected to disclose data breaches). U.S. Attorney Hinds discussed how the federal government “expect[s] [technology] companies [in the Northern District of California] to protect that data and to alert customers and appropriate authorities when such data is stolen by hackers.” Id. See also David Perera & Matthew J. Schwartz, Jury Finds Former Uber CSO Joe Sullivan Guilty of Cover-Up, INFO. SEC. MEDIA GRP. (Oct. 5, 2022), archived at https://perma.cc/UFN9-P58W (discussing specifically what Sullivan’s crime was according to the prosecutors in the Northern District of California). Sullivan committed a crime when he “obstructed an ongoing federal investigation by the Federal Trade Commission into Uber’s data security practices” in the 2014 data breach by not disclosing the 2016 data breach. Id.

88 See Dwyer et al., supra note 86 (noting that there is a preexisting duty to disclose data breaches to the federal government and the DOJ believes “any nondisclosure is a cover-up . . .”). See also Rasch, supra note 62 (describing how a company is not legally required to tell the FTC about a different breach that they were not investigating).

Essentially, the government is asserting that it is a crime to not tell an agency that is investigating your past activities about current activities that the investigator might deem relevant. Importantly, it was not the fact that Uber had a reportable data breach that triggered the obstruction charge, but the fact that they simply failed to inform the FTC about a security vulnerability that might have impacted the settlement of the previous breach[.]
was taking place. This justification of the charge opens up a window for many companies to be susceptible to being charged with misprision of felony. Lastly, the charge of wire fraud was based upon Sullivan wiring $100,000 in bitcoin to the hackers. Throughout the multiple investigations of data breaches conducted within Uber since 2014, Joseph Sullivan is the only Uber employee to ever be charged as a result of a data breach at Uber.

89 See Rasch, supra note 62 (describing that the DOJ is charging Sullivan for not reporting the cyberattack on Uber which is considered the crime in this charge). A major question that results from this charge is that do companies have to report when they are a victim of an actual or attempted data breach? Id. See also What Are Bug Bounty Programs, And Why Are They Becoming So Popular?, SEC. JOURNEY (Nov. 16, 2022), archived at https://perma.cc/NA5D-V9B7 (defining what bug bounty programs are and how they are used). “A bug bounty program gives ethical hackers permission to test if an organization’s applications contain certain types of vulnerabilities.” This is an effective way for companies to “identify and fix vulnerabilities” within their cybersecurity at a reduced cost. Id. See Misprision of Felony, LEGALMATCH (Nov. 18, 2022), archived at https://perma.cc/Y73V-S4JV (detailing what constitutes Misprision of felony). “Misprision of felony is a crime committed when a person knows that someone has been involved in a felony but fails to report it to law enforcement authorities.” Id. “In the U.S . . . it has never been adopted as a crime by most states” and if it has “it is almost never prosecuted[.]” Id. 90 See Dwyer et al., supra note 86 (pointing out that “[a]ny company experiencing a ransomware event is aware of a felony.”). “Therefore, companies need to be very careful that any actions they take cannot be construed as affirmative concealment of that felony.” Id. The DOJ believed the most aggravating factor in this charge is that Sullivan never obtained the true identity of the hackers, but he still paid them. Id. However, it is very common in most ransomware attacks that companies do not know the true identity or names of the hackers and pay the ransom regardless. Id. See also Misprision of Felony, supra note 89 (highlighting that misprision of felony is considered “excessively harsh” therefore it is rarely adopted or utilized in the U.S.). See also Mario Ayoub et al., Lessons from DOJ’s First Prosecution of a Company Executive Covering Up a Data Breach, ALSTON & BIRD (Oct. 11, 2022), archived at https://perma.cc/J9H2-WRKH (highlighting how the misprision theory is the “most troubling aspect of this case.”). “Any company experiencing a ransomware event is aware of a felony; therefore, companies need to be very careful that any actions they take cannot be construed as ‘affirmative concealment’ of that felony.” Id.

91 See Lindsey O’Donnell-Welch, CISOS Navigate Legal Risks After Former Uber Executive’s Conviction, DECIPHER (Apr. 28, 2023), archived at https://perma.cc/W7HR-XSBS (pointing out that the three counts of wire fraud Sullivan was charged for related to paying off the hackers “under the guise of a bug bounty reward[,]”). Before they tried the case, prosecutors dismissed the wire fraud charges due to the lengthy time in prison Sullivan would potentially have to face if found guilty. Id.

92 See Lakshmanan, supra note 76 (detailing that the CEO of Uber at the time, Travis Kalanick, actually approved of “Sullivan’s strategy for handling the unauthorized
During the trial, Sullivan and his lawyers pointed out that Uber isolated him from the company and portrayed him as a “bad apple” in order to separate the corporation from the 2016 data breach. Many Uber executives, including the CEO at the time, were involved in addressing the breach and concealing it because they did not want it to go public. Even Uber employees aware of the data breach testified that those within Uber did not feel as though this was a legitimate cover-up situation. Those employees who did testify against Sullivan, such as Craig Clark, did so to be granted immunity. Clark was a member of the security group that handled the breach, drafted the nondisclosure agreement provided to the hackers, and personally

intrusion[,]’ although Kalanick has yet to be charged). See also Joel Rosenblatt, Uber’s former security chief convicted of data hack coverup, L.A. TIMES (Oct. 5, 2022), archived at https://perma.cc/GD3X-A852 (pointing out that even though Sullivan shared the details of the breach with numerous employees twelve hours after it occurred, he was the only person to be charged for the coverup). 93 See Bonnie Eslinger, Uber Threw Ex-Security Chief Under Bus, Ex-PR Exec Testifies, LAW360 (Sept. 29, 2022), archived at https://perma.cc/U2S9-FF5C [hereinafter Uber Threw Ex-Security Chief Under Bus] (describing how a high ranking public relations professional at Uber, Melanie Ensign, believed that it was unfair how Uber portrayed Sullivan). Ensign stated that Uber likely portrayed Sullivan as a bad apple to “remove that bad apple from the situation and distance the company from the issue that they are accused of . . . .” Id.

94 See Lawler, supra note 83 (discussing how the former CEO of Uber knew about the 2016 data breach when it occurred). Travis Kalanick, then-Uber CEO and the current chief privacy lawyer, knew about the data breach when it occurred, however, was not legally prosecuted. Id.

95 See Rosenblatt, supra note 92 (pointing out that Joseph Sullivan shared information about the data hack as soon as twelve hours after it occurred). Sullivan even informed the CEO at the time, Travis Kalanick, of the data breach. Id. Sullivan’s attorney highlighted this in his closing argument that “Mr. Sullivan could not have reported this to someone higher up at the company.” Id. See also Uber Threw Ex-Security Chief Under Bus, supra note 93 (discussing how an Uber employee, Ensign, felt that Sullivan was not intentionally trying to keep the 2016 data breach a secret within Uber). Another Uber employee, Mat Henley, testified that after Uber fired Sullivan, he “gave a presentation to the rest of the company’s security group . . . stating that numerous people at Uber had been pulled in to deal with the hacking, and ‘We never felt anything was being covered up.’” Id.

96 See Robert Freedman, Ex-Uber lawyer’s immunity in coverup rests on he-said, she-said conflict, LEGAL DIVE (Sept. 15, 2022), archived at https://perma.cc/TR6D-ED4W (discussing how Craig Clark, a previous Uber lawyer, testified against his former boss in order to receive immunity). Even though Clark was the individual who “proposed a plan to have the two hackers join the [bug bounty] program[,]” he was never charged for his involvement. Id.
lied to outside counsel about the 2016 breach.\textsuperscript{97} The prosecution rested on Clark’s testimony which ultimately determined, among other things, the unfortunate outcome of the case.\textsuperscript{98}

Sullivan was found guilty in October of 2022 for obstructing the FTC’s investigation and misprision of felony.\textsuperscript{99} Sullivan now faces a maximum sentence of eight years in prison in addition to a hefty amount of fines.\textsuperscript{100} The two hackers of the 2016 data breach were eventually discovered and prosecuted, ultimately pleading guilty in October of 2019.\textsuperscript{101} As a company, Uber agreed in 2018 to pay $148

\textsuperscript{97} See Dinzeo, supra note 81 (discussing how Clark initially lied about not writing or editing a provision in the NDA). During the trial Clark finally admitted he “made a critical edit to a provision in the agreement” and was not fully truthful when discussing his involvement in the 2016 data breach with prosecutors. \textit{Id.}

\textsuperscript{98} See Bonnie Eslinger, \textit{From ‘Golden Boy’ To Guilty: Snapshots Of Uber Exec’s Trial}, LAW360 (Oct. 6, 2022) [hereinafter From ‘Golden Boy’ To Guilty], archived at https://perma.cc/3T29-MMM9 (pointing out that Clark’s testimony was key for the prosecution to have a strong case against Sullivan). Clark himself originally lied to outside counsel from WilmerHale about the data breach and “came up with the idea to use an exemption within California’s data reporting laws that allows a company to not report disclosures that are made to employees, contractors and agents for a company.” \textit{Id.} However, this information was not discovered until Sullivan’s lawyers provided proof that Clark was the individual who drafted certain key parts of the non-disclosure agreement during the trial. \textit{Id.}

\textsuperscript{99} See Metz, supra note 16 (highlighting that Joseph Sullivan was found guilty on October 5\textsuperscript{th}, 2022 “by a jury in federal court on charges that he did not disclose a breach of customer and driver records to government regulators.”). “The jury found Mr. Sullivan guilty on one count of obstructing the F.T.C.’s investigation and one count of misprision, or acting to conceal a felony from authorities.” \textit{Id.} It only took nineteen hours for the jury to reach a verdict. \textit{Id.}

\textsuperscript{100} See Perera & Schwartz, supra note 87 (portraying how Sullivan “faces up to eight years in prison and $500,000 in fines”). \textit{See also} Ryan Naraine, \textit{Former Uber CISO Joe Sullivan Found Guilty Over Breach Cover-Up}, SECURITY\textit{WEEK} (Oct. 5, 2022), archived at https://perma.cc/EV8A-XT6N (discussing how Sullivan faces “[a] maximum of five years for the obstruction charge, and a maximum [of] three years for a misprision charge.”).

\textsuperscript{101} See Whittaker, supra note 76 (describing how the two hackers, Vasile Mereacre and Brandon Glover were indicted on separate hacking charges related to their hacking of Uber and an online learning portal). \textit{See also} Indictment at 2, U.S. v. Glover, 531 U.S. 198, 697 (2018) (No. CR 18-00348) (charging Glover and Mereacre for hacking multiple companies, including Uber). \textit{See also} Press Release: Florida Man And Canadian National Plead Guilty To Hacking/Extortion Conspiracy (Oct. 30, 2019) (on file with author) (discussing how Glover and Mereacre pled guilty for their roles in an extortion conspiracy to Uber and other companies). The two hackers specifically pled guilty to their involvement in “a plot to extract bounties from victim corporations in exchange for the defendants’ promise to delete stolen confidential data[.]” \textit{Id.}
million to settle claims regarding the breach and enter into a twenty-
year consent agreement with the FTC.  

C. Reaction to the Outcome of United States v. Sullivan

This is the first time a company executive has been individually
prosecuted and successfully convicted for a response to a data
breach. Joseph Sullivan, once widely known as a rock star in the
cybersecurity world and one of the first federal prosecutors to work in
the cybercriminal field, now faces sentencing. Sullivan’s renowned
reputation furthers this surprise to many who are astounded that
Sullivan was actually convicted. This shock also stems from the

102 See In re. Uber Tech., Inc., 152 F.T.C. 3054 (Oct. 25, 2018) (detailing
the procedures and orders that the corporation, Uber, must follow as a result of their
multiple data breaches). This ranges from recordkeeping, compliance monitoring, a
payout, and augmented security protocols. Id. See also F.T.C. Press Release:
with author) (elaborating on their settlement with Uber for their “failure to take
reasonable measures to secure both rider and driver data” which resulted in two
breaches at Uber). See Perera & Schwartz, supra note 87 (discussing Uber’s
settlement and agreement with the F.T.C.). Uber agreed to a lengthy “consent
agreement with the FTC prohibiting it from misrepresenting safeguards for consumer
data and charging the company with maintaining a privacy program.”

103 See Menn, supra note 72 (pointing out that this is the “first major criminal case
brought against a corporate executive over a breach by outsiders.”). See also Perera
& Schwartz, supra note 87 (furthering the point that this is the first time a CISO has
been held personally liable for mishandling a data breach). See also Kimberly Peretti
et al., Mitigating the Risks in Era of Heightened Liability for CISOs, BL (Nov. 28,
2022), archived at https://perma.cc/938J-RSZK (highlighting how the violations
Sullivan was charged with was related to concealment for a data security incident).

104 See Hill & Browning, supra note 14 (describing how before entering the corporate
security world in 2002, Sullivan was a federal prosecutor working cybercrime cases).
See also Menn, supra note 72 (discussing how the judge has yet to set a date for
sentencing after Sullivan was found guilty on October 5th). “Sullivan may appeal if
post-trial motions fail to set the verdict aside.” Id.

105 See Menn, supra note 72 (pointing out that Joseph Sullivan was a prominent
security expert that worked at Facebook, Uber, and Cloudflare). See Perera &
Schwartz, supra note 87 (discussing how this case is so instrumental partly due to
Sullivan’s “stature and reputation for advancing cybersecurity practices.”). Joseph
Sullivan “served as a federal prosecutor and then CSO of Facebook for five years.
He was also a commissioner on President Barack Obama’s Commission on
Enhancing National Cybersecurity, which recommended ways to improve the
nation’s cybersecurity.” Id. Many within the cybersecurity industry have been
outspoken for supporting Sullivan and exclaimed this case as “tribalism.” Id.
fact that so many other employees of Uber, in-house attorneys, and C-level executives who knew about the 2016 breach were never held accountable for their knowledge or actions.\textsuperscript{106} It is concerning to many that full liability has fallen on Sullivan even though it is common for CISOs to be heavily involved during an investigation of a data breach and none of the other countless employees and executives who knew about the breach.\textsuperscript{107} This case presents a confusing potential precedent, where members of a company may be liable for breaches similar to that of the 2016 Uber breach.\textsuperscript{108} The line is now blurry in

\textsuperscript{106} See From ‘Golden Boy’ To Guilty, supra note 98 (pointing out how Sullivan believed he was scapegoated by Uber and Uber’s attorney, Craig Clark). See also Rosenblatt, supra note 92 (pointing out that “Uber’s legal department and other managers were aware of the incident before it blew up publicly.”). Sullivan’s attorney highlighted the notion that Sullivan reported this breach to the highest person at the company, the CEO, therefore he was not trying to cover up this breach. Id. Other higher up employee’s and lawyers’ knowledge of the breach should have been taken into account. Id. See also Jody R. Westby, Uber Trial: A Lost Opportunity For Cyber Governance, FORBES (Oct. 8, 2022), archived at https://perma.cc/5JZW-J75C (discussing how the case sent “chills up the spines of CISO/CSOs.”). See also David Jones, Uber ex-CSO verdict raises thorny issues of cyber governance and transparency, CYBERSECURITYDIVE (Oct. 19, 2022), archived at https://perma.cc/Q8KM-R85H (describing how “Uber in July entered a non-prosecution agreement with DOJ, which allowed upper management to avoid charges . . . ”).

\textsuperscript{107} See Menn, supra note 72 (quoting Dave Schackleford, discussing that “[p]ersonal liability for corporate decisions with executive stakeholder input is a new territory that’s somewhat uncharted for security executives . . . ”). This creates concerns that company decisions to not disclose a data breach would have personal repercussions for security executives. Id. See also Perera, supra note 87 (pointing out that CISOs are now questioning why others are not being held accountable for this cover up). During Sullivan’s case his defense argued that the company’s legal team would be accountable for reporting this data breach and not Sullivan. Id. See also From ‘Golden Boy’ To Guilty, supra note 98 (describing how Sullivan believed it was up to attorneys to report the data breach, if necessary). Sullivan specifically told outside counsel from WilmerHale that “he didn’t have a role in the disclosure decision because that was up to Clark and the legal department . . . ” Id.

\textsuperscript{108} See Eduard Kovacs, Industry Reactions to Conviction of Former Uber CSO Joe Sullivan: Feedback Friday, SECURITYWEEK (Oct. 7, 2022), archived at https://perma.cc/P5MQ-ZRAB (utilizing opinions from a variety of CISOs at major corporations to discuss the potentially dangerous repercussions of this case). The CISO of JupiterOne believes that

[i]his case has set a terrible precedent that creates confusion around who should take liability for decisions during an incident response event. In this particular case, it was clear that Joe Sullivan coordinated his actions with the blessing of executive management, yet Joe was the one that ended up holding the bag.
terms of who and when someone should be held accountable under the circumstances for covering up a data incident and not reporting it. 109

D. SEC’s Reaction to Recent Data Breaches

The Securities and Exchange Commission (SEC) has taken a different approach to handling data breaches compared to the FTC. 110 The SEC concentrates on both ensuring that markets are fair for all consumers and also provides general oversight for regulating securities markets. 111 This oversight includes monitoring cybersecurity-related business activities for companies internally and externally. 112 The SEC conducts this work through centering on companies and individuals within the companies through cases such as FTC v. Equifax Inc. (“Equifax”), which specifically highlights the different roles that the SEC and FTC take when addressing data breaches. 113

Id. See also Jones, supra note 106 (describing how the line “between a ‘coverup’ and a failure to report an incident” is now blurred due to this conviction).

109 See Mario Ayoub et al., supra note 90 (discussing how this case may have unprecedented effects on the “line between ‘covering up’ a data incident and merely declining to report it.”).

110 See Andrew Chung & Nate Raymond, U.S. Supreme Court leans toward making challenges to FTC and SEC easier, REUTERS (Nov. 7, 2022), archived at https://perma.cc/SX79-NGMF (comparing and contrasting the SEC and FTC’s roles).

111 See The Role of the SEC, INVESTOR.GOV (Feb. 22, 2023), archived at https://perma.cc/4V7R-BDTG (defining the mission and purpose of the SEC). The SEC “has a three-part mission: [p]rotect investors[,] [m]aintain, fair, orderly, and efficient markets[,] and [f]acilitate capital formation[.]” Id. This ensures that “[c]ompanies offering securities for sale to the public must tell the truth about their business, the securities they are selling, and the risks involved in investing in those securities.” Id.

112 See Aaron Charfoos & Jacqueline Cooney, SEC Proposed Cybersecurity Rules – What They Are and What Our Clients Should be Doing Now, JDSUPRA (Oct. 11, 2022), archived at https://perma.cc/C96G-J7WV (describing how the SEC monitors different activities of companies). The SEC monitors cyber-related business activities internally through keeping watch of the Board of Directors oversight of cybersecurity. Id. While the SEC also analyzes public companies’ activities which externally affect consumers in the market. Id.

In Equifax, personal information of over 40 percent of the U.S. population or 147 million consumers was compromised in 2017.\textsuperscript{114} The company failed to implement basic security measures and suffered the consequences when the FTC and SEC both became involved in suits against the company and individuals within Equifax.\textsuperscript{115} While the FTC focused on holding the company accountable as a whole through reaching a settlement with the company to pay at least $575 million, the SEC rather centered on holding certain executives accountable for knowing about the breach and conducting insider trading before disclosing the breach.\textsuperscript{116} The SEC charged and


\textsuperscript{114} \textit{See Josh Fruhlinger, Equifax data breach FAQ: What happened, who was affected, what was the impact?}, CSO (Feb. 12, 2020), archived at https://perma.cc/ED6N-CBUN (detailing the Equifax breach). Equifax was hacked initially through a vulnerability in the consumer complaint portal which was supposed to have been fixed by Equifax employees but had yet to be. \textit{Id.} “The attackers pulled data out of the network in encrypted form undetected for months because Equifax had crucially failed to renew an encryption certificate on one of their internal security tools.” \textit{Id.} \textit{See also Sarah O’Brien, Consumers are getting payments from Equifax data breach settlement. Here’s what to expect if you filed a claim}, CNBC (Dec. 28, 2022), archived at https://perma.cc/CF2Z-QA9D (pointing out how many people’s data was affected from Equifax’s data breach which occurred in 2017).

\textsuperscript{115} \textit{See Fruhlinger, supra note 114} (pointing out how Equifax could have prevented the extensive damage from the data breach if they maintained proper data governance practices). Equifax failed to discover an expired certificate which would have inspected encrypted traffic and likely have discovered the hackers. \textit{Id.} \textit{See also Equifax to Pay $575 Million as Part of Settlement with CFPB, and States Related to 2017 Data Breach, supra note 113} (describing the FTC’s case against Equifax). \textit{See also SEC Charges Three Chicago-Area Residents with Insider Trading Around Equifax Data Breach Announcement, supra note 113} (describing the SEC’s suit with three former employees of Equifax).

\textsuperscript{116} \textit{See Stipulated Order for Permanent Injunction and Monetary Judgment, at 1–2, FTC v. Equifax Inc., N.D.G.A. Dist. Ct. (2019) (No. 1:19-cv-03297-TWT)} (explaining the complaint, order for injunction, and monetary judgment). \textit{See also Equifax to Pay $575 Million as Part of Settlement with CFPB, and States Related to 2017 Data Breach, supra note 113} (pointing out that Equifax “agreed to pay at least $575 million, and potentially up to $700 million, as part of a global settlement with
Data breaches frequently result in convictions of multiple executives, including Equifax’s former Chief Information Officer, for insider trading. The SEC has an interest in protecting consumers from data breaches due to the adverse effects cybersecurity incidents have on a company’s revenue and consumers’ investment in the company’s stock. Since consumers typically do not consider or have adequate knowledge of a company’s cybersecurity vulnerabilities when choosing where to invest their money, the SEC steps in to fill this void through monitoring companies’ cybersecurity governance. The SEC is upping fines against companies and their cybersecurity regulations in order to necessitate companies’ executives and boards maintain stringent cybersecurity guidelines to fully protect consumers.

---

117 See Former Equifax employee sentenced for insider trading, DOJ (June 27, 2019), archived at https://perma.cc/YVE3-3FWP (describing the charges against Jun Ying, former Chief Information Officer of Equifax). Ying delayed the public disclosure of the data breach and participated in insider trading after news of the data breach to Equifax. Id.

118 See Jennifer Gregory, What the SEC Requires From Businesses After a Data Breach, SEC. INTEL. (Nov. 29, 2021), archived at https://perma.cc/9XCM-CESD (describing how the SEC takes many steps to ensure that “consumers are not investing their hard-earned money in a company’s stock based on false or misleading information.”). See also John Zorabedian, What’s New in the 2021 Cost of a Data Breach Report, SEC. INTEL. (July 28, 2021), archived at https://perma.cc/L64V-KBUE (noting how the average cost of a “data breach increased by nearly 10% to $4.24 million, the highest ever recorded.”). The increasing cost of data breaches makes investments for consumers riskier than they realize. Id.

119 See Gregory, supra note 118 (pointing out cybersecurity governance significantly affects a company’s revenue, therefore when a company faces a cybersecurity incident, the price of their stock typically drops). Id. Since “consumers don’t have cybersecurity-related information when they purchase company stock . . . their investment [is] much riskier than they realize.” Id.

120 See id. (highlighting how the “SEC is leveraging fines to companies with poor cybersecurity practices more and more.”). See also Bob Ackerman, New SEC Cybersecurity Reporting Requirements: Three Things Companies Need To Do Now, FORBES (May 25, 2022), archived at https://perma.cc/M6Y2-8D8J (describing the
Through ensuring vigorous cybersecurity governance from companies, the SEC encourages a transparent and effective governance within a company.\textsuperscript{121} The development of the SEC’s role in cybersecurity incidents is a positive transformation for preventing cyberattacks and decreasing the pressure CISOs face as it disperses the cyber responsibility in a company.\textsuperscript{122}

IV. Analysis

A. A Wasted Opportunity by the Federal Government

The prosecution and conviction of Joseph Sullivan was a missed opportunity by the DOJ, as they relinquished a chance to establish a paradigm for executives of companies to follow proper cybersecurity governance guidelines.\textsuperscript{123} The countless executives, officers, and board members that either knew or should have known SEC’s proposed rules and amendments that seek to bolster company’s defense against cyberattacks). These rules “aim to standardize disclosures of material cybersecurity incidents and improve visibility into a company’s cybersecurity risk management and governance policies to better inform investors.” \textit{Id.}  

\textsuperscript{121} See generally \textit{How CISOs and boards can prepare for the new era of cyber transparency}, PwC (Feb. 23, 2023), \textit{archived at} https://perma.cc/V2PT-VD3U (pointing out how not only CISO’s have to prepare for these new regulations, boards must also work on their involvement in cybersecurity governance as well).  

\textsuperscript{122} See \textit{SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies}, SEC (Mar. 9, 2022), \textit{archived at} https://perma.cc/8V8W-ERDJ (noting how the proposed amendments to the SEC’s rules will “standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies.”). \textit{See also Sergiu Gatlan, SEC wants public companies to report breaches within four days}, \textit{BleepingComputer} (Mar. 10, 2022), \textit{archived at} https://perma.cc/7Q5X-E6MD (describing the newly proposed rules that the SEC will implement in the near future).  

\textsuperscript{123} See Westby, \textit{supra} note 106 (explaining how U.S. v. Joseph Sullivan was decided wrongly because the federal government should have been targeting Uber’s board, C-suite, and officers). \textit{See also} Menn, \textit{supra} note 72 (discussing how Sullivan kept multiple executives aware of the data breach).  

While he directed the response to the two hackers, many others at the company were in the loop, including a lawyer on Sullivan’s team, Craig Clark. Evidence showed that Sullivan told Uber’s then-chief executive, Travis Kalanick, within hours of learning about the threat himself, and that Kalanick approved Sullivan’s strategy. The company’s chief privacy lawyer, who was overseeing the response to the FTC, was informed, and the head of the company’s communications team had details as well.  

\textit{Id.}
about the 2016 data breach is unsettling.\textsuperscript{124} Centering solely on Joseph Sullivan is a grave mistake because the government could have set the example the cybersecurity world needs, poor management and lack of board oversight of cybersecurity regulations will result in serious repercussions.\textsuperscript{125} Even though Sullivan may have been to blame for the concealment of the data breach, the CEO of Uber and other senior management who had knowledge of the breach were the ones who ultimately should have made a formal breach disclosure and have been held accountable, not Sullivan.\textsuperscript{126} Similarly, Uber’s board lacked a proper reporting and monitoring system during the 2016 data breach portraying a major failure in the company’s management of

\textsuperscript{124} See Jones, \textit{supra} note 106 (highlighting the confusion of why “other senior executives, C-suite officials and corporate board members” were not charged when Sullivan was convicted). A CISO at OneSpan, Christian Vezina, is quoted, “[w]hen a major security incident hits, there is a collective effort between executives and the security team to address, mitigate and contain it.” \textit{Id}. Therefore, “[i]f a decision was made to limit the information disclosed about the incident, Vezina argues the CISO was not acting alone.” \textit{Id}. See also Rosenblatt, \textit{supra} note 92 (exposing that Sullivan had shared the data breach with numerous employees when it first occurred). Sullivan even disclosed it to the “top person at Uber” the Uber CEO at the time. \textit{Id}. See Westby, \textit{supra} note 106 (pointing out that the Uber Board “should have been exercising oversight” and the directors and officers “should have been managing cyber risks.”). See also Menn, \textit{supra} note 72 (pointing out that “[m]ost security professionals had been anticipating Sullivan’s acquittal” because he kept other executives such as the CEO informed of the breach).

\textsuperscript{125} See Perera & Schwartz, \textit{supra} note 87 (explaining that “no one else involved in Uber’s response has been charged in connection with the data breach or alleged cover-up.”). Generally, it is “legal’s role . . . to provide advice to the executive(s) who make the decision” to not disclose the breach. \textit{Id}. See Westby, \textit{supra} note 106 (explaining how the federal government had a proper opportunity to hold directors and officers accountable for mishandling a data breach).

\textsuperscript{126} See Dinzeo, \textit{supra} note 81 (elaborating on who knew or were thought to have known about the Uber data breach). “Exactly how much Uber’s c-suite knew about the breach remains murky. Clark said Sullivan had told the security response team that he was communicating directly with CEO Travis Kalanick and other members of the ‘A-Team.’” \textit{Id}. See also Westby, \textit{supra} note 106 (pointing out that it was Kalanick’s decision and “possibly other senior management not to make a formal breach disclosure” and not Joseph Sullivan). See also Peretti et al., \textit{supra} note 103 (describing proactive steps companies should take to protect against liability for future data breaches). Companies must provide assistance to CISOs regarding the everchanging disclosure considerations, maintaining consistent contact with counsel and board, and ensuring there is a response plan for a data breach among other things. \textit{Id}. 
cybersecurity risks. The federal government lost an opportunity to prosecute directors and officers of Uber for concealment and failure to report a data breach, which would have been a model case for holding C-level executives, officers, and board members accountable as a whole for their role in cybersecurity and maintaining efficient governance systems within companies.

The outcome of this case perpetuates the notion that the CISO is the scapegoat for any and all cyber security event. Prosecuting Sullivan only incentivizes CISOs to minimize future cyberattacks in this fear-based system. Future convictions following this trend will further propagate cyber risks and weaken cybersecurity programs in companies, regardless of their size or notoriety. The CISO must

127 See Westby, supra note 106 (highlighting how Uber did not have “a cyber governance framework in place that would have informed them about the hack so it could be appropriately handled and reported.”). See also Bhuiyan, supra note 16 (pointing out how “[s]ome have questioned whether the role of other company executives and its board should be investigated as well . . . .”).

128 See Westby, supra note 106 (describing how Sullivan’s case “was the wrong result and a lost opportunity for the federal Government to send a real message . . . .”). “It was the wrong result because it was the wrong case: it laid blame on the [CISO] instead of the company’s directors and officers (D&Os).” Id. This was the perfect opportunity for the DOJ to finally hold board members and top executives accountable for such a data breach that the federal government has been looking to legally pursue. Id.

129 See Peretti et al., supra note 103 (pointing out that “CISOs have become a new target in civil and criminal litigation . . . .”). See also Armstrong, supra note 70 (highlighting that “21 percent of IT decision-makers would most likely blame a data breach on the CISO . . . .”). “CISOs are an incredibly important resource, but all too often they find themselves the scapegoat in the event of a data breach.” Id. See also Kochman, supra note 69 (highlighting how “[i]t would be very naïve to believe that other executives haven’t done the exact same thing that Joe Sullivan” did).

130 See Menn, supra note 72 (describing how it is a commonality for CISOs to pay off hackers and conceal data breaches from the public due to the complex pressure put on CISOs). This case “may be one of the last: In the five years since Sullivan was fired, payoffs to extortionists, including those who steal sensitive data, have become so routine that some security firms and insurance companies specialize in handling the transactions.” Id. See also Dwyer et al., supra note 86 (discussing how this case is complicated as “it blurs the line between covering up a data incident and merely declining to report it.”). Since there is no transparent regulation for reporting data incidents, CISOs will be incentivized to de-emphasize future data breaches for fear of being prosecuted. Id.

131 See Sabin, supra note 14 (pointing out the difficulties that CISOs face in their complex role and how this decision “could dissuade people from CISO roles in the future.”). “CISOs face a more challenging threat and regulatory environment than they did six years ago when Sullivan’s offense happened, including a growth in
stop being seen as a scapegoat for cybersecurity incidents especially when multiple executives are aware of a breach, and there is no formal cyber governance system established at the company. The 2016 data breach was not a particularly unusual situation, even if the FTC was already investigating a previous breach at Uber, as this could happen to any company or CISO. Consequently, this case should be of great concern to current and future CISOs, as this is not the precedent that any company or executive wants to establish.

Potential dissuasion from this role augments dangers in cybersecurity and leads to heightened risks in handling future data breaches. See Newman, supra note 68 (describing how CISOs are considered “chief scapegoat officers”). CISOs handle the challenges of managing massive organizations and it is “inevitable that companies suffer hacks and breaches, and [CISOs] preside over the aftermath.” See Menn, supra note 72 (pointing out how this finding will result in “increased skepticism about infosec overall.”). See also Burgess, supra note 11 (pointing out how CISOs need proper company governance regarding cybersecurity to be able to efficiently perform their job). “Today’s CISO cannot and will not be successful in his or her efforts without buy-in from both the corporate leadership team and those who are most affected by the information security policies and procedures: the operations teams.”

See Mishra, supra note 12 (describing how CISOs are commonly blamed for data breaches). “[I]t seems like CISOs are the ones that ultimately take the fall for a data breach, no matter how it may have happened.” See also Freedman, supra note 96 (explaining how Sullivan acted in accordance to how a typical CISO would act in such a situation and did not “direct anyone to be misleading.”). Sullivan’s counsel points out that “[y]ou won’t hear a single witness take that stand and say that Joe Sullivan told them to lie to the FTC or destroy documents or hide what had happened from Uber’s senior management or the Uber legal team . . . .” The testimony in the case portrays how Sullivan did inform the senior management and Uber legal team of the data breach and it was the decision of the higher up’s to not disclose the breach to the public. See also Former Uber CISO Convicted: What, How, & Why?, supra note 70 (pointing out that “[c]yber-attacks happen to everyone and all the time” therefore future breaches which mirror this one are inevitable).

See Mishra, supra note 12 (taking specific accounts from CISOs about who should take the blame for data breaches). A former CISO at Twitter pointed out that “CISOs don’t have the unilateral authority for decisions outside of the infosec department and if a potential risk is found due to activity in another area of the business, they can only advise on the proper course of action.” See also Westby, supra note 106 (pointing out why this case should be of concern to not only companies, but also the American public).

The conviction did not send tremors through board rooms across America, but it did send chills up the spines of CISO/CSOs. It was
B. The Federal Government Must Positively Incentivize the Open Discussion of Data Breaches

Contrary to pursuing criminal prosecution of CISOs such as Joseph Sullivan, the federal government and organizations such as the FTC and SEC should instead focus on instituting transparent cybersecurity rules and reporting requirements that stress the importance of cyber-governance within companies. Any future rules, requirements, and legislation should emphasize the necessity of monitoring and reporting when evaluating cyber risks and the importance of the roles directors, officers, and the board must take on cyber oversight. The federal government has recently implemented legislation in this area, as President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (“CIRCIA”), which will require covered entities to report certain cyber incidents and ransomware payments to the Cybersecurity & Infrastructure Security Agency (CISA). CISA will then work to supply resources, assist

the first time a CISO/CSO has been held criminally liable for their actions in managing a cyber attack. Until companies treat cyber as an enterprise risk and make business units responsible for the systems and data they use, cybersecurity programs will continue to lag and CISO/CSOs will be incentivized to minimize – or lie about – cyber attacks. That should scare America because our current state of cybersecurity plays a key role in national and economic security.

Id.

135 See Menn, supra note 72 (highlighting how the SEC is pushing for more disclosure of data breaches). See also Dwyer et al., supra note 86 (pointing out how at the time of Sullivan’s action “there was no generally applicable statute requiring companies to disclose data security incidents to the federal government.”). There is a clear need for such regulation if the federal government is seeking to prosecute individuals for failing to report data breaches in a timely manner. Id. See also Security Beyond Prevention: The Importance of Effective Breach Disclosures, supra note 56 (describing how the FTC relies on broad laws either from the state, federally, or from a vague law in Section 5 of the FTC Act).

136 See Jones, supra note 106 (describing how “[c]ompanies should have a written response plan and stick to the plan” when cybersecurity incidents occur). See also Westby, supra note 106 (delineating what regulations the government should implement in order to clarify current disclosure and data breach law).

137 See CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022 (CIRCIA), supra note 86 (elaborating on the procedures to be followed under CIRCIA). “These new authorities are regulatory in nature and require CISA to complete mandatory rulemaking activities before the reporting requirements go
victims of cyber-attacks, and provide advice to companies to protect from further, similar cyber incidents.\textsuperscript{138} CIRCIA has emphasized the protections it will grant entities who report cyber incidents or ransom payments in order to encourage such reporting.\textsuperscript{139} This method of incentivization is a constructive push in modifying the government’s current penalizing manner of handling companies who disclose cybersecurity incidents.\textsuperscript{140}

There is also a positive progression happening at the SEC level to establish such rules, as they are in the process of finalizing legislation which would provide transparency to a clouded and outdated compilation of regulations used to monitor cybersecurity.\textsuperscript{141}

\begin{footnotesize}
\textsuperscript{138} See Dwyer et al., supra note 86 (pointing out that CIRCIA will not “take effect until the U.S. Department of Homeland Security finalizes implementing regulations, likely in 2025.”). See \textit{CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022 (CIRCIA)}, supra note 86 (describing how CIRCIA will work with CISA to help entities who are affected by the data breach and the consumer victims).
\textsuperscript{139} See Borgia, supra note 86 (describing how “the law also includes significant legal protections for information provided in cyber incident and ransom payment reports— including those submitted voluntarily[].”)
\textsuperscript{140} See id. (specifying the protections CIRCIA provides for companies who report cyber incidents and ransom payments). Some of these protections include “[i]nformation shared by DHS and CISA from reports of covered cyber incidents or ransom payments shall be anonymized as not to identify the victim. Information may not be used in any federal, state, local, or tribal enforcement proceeding against he covered entity.” Id. “No cause of action shall lie in any court for the submission of information under CIRCIA.” Id. “No report submitted under CIRCIA, or any communication or material prepared for the sole purpose of preparing, drafting or submitting a report, may be received in evidence, subject to discovery or otherwise used in any legal proceeding.” Id.
\textsuperscript{141} See Pearlson & Hetner, supra note 86 (describing the SEC’s proposed rule, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure).
\end{footnotesize}
The SEC is focusing their proposed set of rules and amendments on internal governance capabilities that detail management’s role and the company board’s oversight of cyber risks. This newly proposed legislation would also require regular and timely disclosures of cybersecurity incidents from public companies in order to keep investors fully informed. This is a significant and productive change for the protection of CISOs as these clear rules would legislatively mandate board’s to be considerably involved in their company’s cybersecurity policies and procedures. Therefore, making CISOs and company boards work together to augment the company’s cybersecurity governance, requiring the board to be the ultimate overseer of the CISO’s cyber risk strategy.

Alternatively, while the FTC has focused on setting precedents through previous case law and creating de facto requirements, they still have struggled to implement unambiguous legislation pertaining to cybersecurity protections similar to that being enacted by the federal government and the SEC. The FTC continues to stray from the real

“The SEC will soon require companies to disclose their cybersecurity governance capabilities, including their board’s oversight of cyber risk, a description of management’s role in assessing and managing cyber risks, the relevant expertise of such management, and management’s role in implementing the registrant’s cybersecurity policies, procedures, and strategies.”

See id. (pointing out how board members will have a “[c]ybersecurity [a]ttitude [a]djustment” to comply with the SEC’s proposed rule). “To provide proper oversight and comply with the regulatory environment, board members are going to have to up their cybersecurity game. It’s no longer adequate to just hear about the protections put in place, or the results of the latest phishing exercise.”

Highlighting how “most board members believe it’s not a matter of if, but when their company will experience a cyber event.”

See Gatlan, supra note 122 (noting how the SEC’s revised rules and new regulations would require companies to disclose “measures taken to identify and manage cybersecurity risks” on the 8-K form four days after a cyber incident occurs).

See How CISOs and boards can prepare for the new era of cyber transparency, supra note 121 (explaining how the SEC’s revised rules and regulations expand disclosures for the board and management). Boards must now “address whether it needs cyber expertise to effectively oversee this risk” of cybersecurity within their group.

See id. (pointing out how CISOs and boards must work hand in hand to effectively create a cybersecurity governance which meets the SEC’s new standard). While “CISOs should think through their communication frequency and content with boards and CEOs to ensure they’re addressing key cybersecurity risks.”

See Security Beyond Prevention: The Importance of Effective Breach Disclosures, supra note 56 (pointing out that the main source of information the FTC relies on is through cases, business guidance resources, and sometimes “de facto breach
issue it has been trying to address for almost twenty years; strengthening cybersecurity regulations.\(^{147}\) The FTC should follow the SEC’s footsteps of instituting new legislation which would ensure that the blame does not fall exclusively on the CISO.\(^ {148}\) This legislation should emphasize how the board and other top executives must oversee cybersecurity strategies and governance of their company’s.\(^ {149}\)

The CISO must not be the only executive in charge of such a hefty duty as cyberthreats continue to increase and companies cybergovernance and support network is not strong enough to combat these cyber risks.\(^ {150}\) Creating regulations such as these would be instrumental in augmenting cybersecurity governance and remove the flawed notion that CISOs are scapegoats.\(^ {151}\)

disclosure requirement[s]). De facto breach disclosure requirements are an opaque methodology of prosecuting companies as there is not a clear and specific law for one to follow. Id.\(^ {147}\) See id. (describing how the FTC relies on “state breach notification laws and sector-specific federal breach notification laws [to] require disclosure of some breaches.”). If none of these laws apply, the FTC then relies on Section 5 of the FTC Act which notes that if “a breached entity that fails to disclose information to help parties mitigate reasonably foreseeable harm” will violate the FTC Act. Id. Relying on this broad law is not an effective monitoring method as it provides confusing legal obligations for companies handling disclosures as “accurate and timely” are not specific requirements that a company can ensure they are following to their best ability. Id.\(^ {148}\) See Pearlson & Hetner, supra note 86 (describing the SEC’s newly proposed rule titled “Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.”). This legislation will include the requirement for “companies to disclose their cybersecurity governance capabilities, including the board’s oversight of cyber risk, a description of management’s role in assessing and managing cyber risks, the relevant expertise of such management, and management’s role in implementing the registrant’s cybersecurity policies, procedures, and strategies.” Id.\(^ {149}\) See id. (describing how “board members are going to have to up their cybersecurity game” to align with advancing legislation). “Board members must take the position that cyber attacks are likely, and exercise their oversight role to ensure that executives and managers have made proper and appropriate preparations to respond and recover.” Id.\(^ {150}\) See id. (describing how “about one third of board members say they interact with the CISO only when he/she is presenting to the board.”). There needs to be significant change to augment collaboration between the board and the CISO in order to properly combat cyber threats and decrease the amount of responsibility the CISO is unfairly designated. Id.\(^ {151}\) See Westby, supra note 106 (describing why it is so important to determine the proper positions which should be held accountable for mishandling data breaches in
Alongside the implementation of these new regulations, prosecutors should aide in the advancement of this movement by focusing their efforts on bringing actions against the actual company perpetuating poor governance practices rather than individually targeting CISOs. This would further hold boards accountable by ensuring there is a good faith effort to create a system of monitoring and reporting within the company, and it would additionally make the board responsible for any oversight in this area. This change could have fixed issues seen in Uber’s 2016 board who was unaware of Uber’s poor cybersecurity governance due to their lack of proper oversight of Uber’s cyber sector. It took years for the 2016 Uber data breach to be exposed by a delayed investigation by Uber’s board. This is unfortunately a commonality with many other boards who do not have a secure procedure for reporting, monitoring, and supervising management of CISOs. This prosecution method could a major company). “Spreading responsibility for cyber risks across an organization is not just a best practice; it is the only way cybersecurity programs get implemented in operations and mature.” Id.

152 See Sabin, supra note 14 (pointing out how CISOs typically rely on their organizations’ CEOs and company boards and typically “struggle to see eye to eye”). Since “CISOs often require the buy-in of their chief executive officers and boards to get the staffing and budget they need to properly secure their operations” their role can only be properly accomplished by efficient governance practices. Id. See also Armstrong, supra note 70 (noting that “CISOs can do little to control the company’s reporting structure” as it is in the hands of the executive team and board members).

153 See Burgess, supra note 11 (describing how a “collaborative engagement” and effort is necessary to properly protect from cybersecurity incidents). There should be an alliance of “security policies and procedures and business outcomes” encouraged and instituted by management and boards. Id. See Peretti et al., supra note 101 (explaining how boards should run their companies with cybersecurity in the forefront). CISOs should be informed and supported on disclosure considerations and rules with routine board updates. Id.

154 See Isaac et al., supra note 80 (elaborating on how it took years for the Uber board to address the data breach of 2016). The breach was not publicly disclosed until the former Uber CEO, Kalanick, stepped down and was replaced by Dara Khosrowshahi who conducted significant investigations leading to the disclosure of the 2016 Uber data breach. Id.

155 See id. (pointing out how Uber “discovered the breach as part of a board investigation into Uber’s business practices” long after the breach occurred).

156 See Peretti et al., supra note 103 (explaining how companies need to enhance their monitoring and reporting measures to match advancements in evolving disclosure law). Companies should maintain routine board updates and “review their current directors and officers and cyber policies in tandem with an eye toward potential gaps in CISO liability coverage.” Id. Taking these steps will allow companies to limit company and CISO liability and be in a better position if a cybersecurity incident
be very effective in aiding the general movement to augment cybersecurity in companies and spark real change.¹⁵⁷

C. Larger Companies Should Become Models for Cybersecurity Governance

The prosecution of directors, officers, and board members who are not properly maintaining cybersecurity governance would set proper standards for other companies and startups to follow.¹⁵⁸ Recent holdings and advancements in legislation portray how boards are soon going to have to meet their duty of loyalty and good faith oversight through proper monitoring and reporting of cybersecurity risks.¹⁵⁹
Though this development is still evolving, it is clear there is momentum towards holding top executives, officers, and board members accountable for cybersecurity incidents which were preventable or failed in being disclosed in a timely manner.\textsuperscript{160} Larger companies, therefore, must adapt to this movement and set an example for smaller companies that sturdy cybersecurity governance is only possible through collaboration between the CISO, board, and top executives.\textsuperscript{161} Having companies take on leadership roles by acting as models of cybersecurity governances will teach startups and other companies about proper cyber governance and is an essential consequence of such proposed legislation of the SEC and federal government.\textsuperscript{162} If companies cannot fill this role, than an appropriate case which holds board members and knowledgeable executives accountable for a mishandled data breach, unlike in \textit{U.S. v. Sullivan}, would be an exemplary foundation to remove the notion that a CISO should be treated as a scapegoat for a mishandled data breach.\textsuperscript{163}

V. Conclusion

While there is much progress to be made, the new legislation presented by the federal government and SEC should bring assurance to CISOs that they will be supported by their company, board, and management. Further regulation of companies’ cybersecurity governance will establish a transparent system where CISOs, company

\textsuperscript{160} See \textit{Mishra}, \textit{supra} note 12 (pointing out a commonly held belief that “the executive board . . . is ultimately in charge of governance” and they “should take responsibility for a data breach.”).

\textsuperscript{161} See \textit{Westby}, \textit{supra} note 106 (discussing how companies can maintain a leadership role in the cybersecurity field if they teach startups about cyber governance). Particularly, Uber could have become a model to other companies if they ameliorated their weak cybersecurity governance and disclosed the breach properly. \textit{Id.}

\textsuperscript{162} See \textit{id.} (pointing out how larger companies can act as a proper example, for smaller startups or companies to follow).

\textsuperscript{163} See \textit{id.} (highlighting the importance of correctly prosecuting board members and executives that are directly accountable for their mishandling of cybersecurity). See \textit{also} United States v. Sullivan, No. 20-cr-00337-WHO-1, 2022 U.S. Dist. LEXIS 154594, at *1-2 (N.D. Cal. Aug. 27, 2022) (noting the case which pinned Joseph Sullivan, former CISO of Uber, as a scapegoat for an Uber data breach in 2016).
executives, and boards can follow clearly defined rules that clarify current, ambiguous regulations. Following the trend of these newly imposed rules, a company’s cybersecurity governance should not be attributed solely to the CISO. A company’s board members and management should also be required to take on further responsibility in this matter. The FTC should align with this trend to prevent dissuasion from individuals taking on the challenging role of a CISO. As data breaches continue to augment at an alarming rate, the number of CISOs in companies will only increase. Therefore, having a strong support system within a company will be necessary to properly support the CISO and protect the company, its investors, and its consumers from cybersecurity attacks. Holding CISOs criminally liable is not the solution for minimizing data breaches. Rather, maintaining an open line of communication for monitoring, reporting, and disclosing will work best toward achieving secure cybersecurity governance.