A Practitioner's Guide to Cybersecurity Whistleblowing

Dallas Hammer
Jason Zuckerman
Zuckerman Law
1934 Old Gallows Road
Suite 350
Tysons Corner, VA 22182
dhammer@zuckermanlaw.com
(571) 288-1309 (v)
(202) 888-7555 (f)
https://www.zuckermanlaw.com
blog: https://www.zuckermanlaw.com/whistleblower-protection-law-blog/

I. Introduction

Most people familiar with cybersecurity agree that data breaches have become an issue of grave national concern. If you are an American citizen reading this, more likely than not, you've had some of your personal information compromised.

Data breaches come in many forms – from deficient security controls, to failures to apply the controls, to malicious external attacks from hackers. Even the external attacks are varied. From DNS attacks, to phishing, to viruses – hackers' tools range from unsophisticated to complex, well-hidden plots. Hackers' motivations are similarly diverse. State (or quasi-state) actors look to undermine our national security and steal our sensitive secrets; hacker rings use pilfered, non-public information for insider trading; others are simple conmen looking to bilk unsuspecting individuals out of their life savings – either through promises of getting rich quick, ransomware, or any other number of scams new and old.

In the past few years, we have witnessed massive breaches of systems we once thought were the among the most secure. For example, in June 2015, the U.S. Office of Personnel Management ("OPM") revealed that it had suffered a data breach pertaining to the records of as many as 18 million people. Barrett, Devlin, *U.S. Suspects Hackers in China Breached About four (4) Million People's Records, Officials Say*, Wall Street Journal (June 5, 2015); Perez, Evan and Prokupecz, Shimon, *First on CNN: U.S. data hack may be 4 times larger than the government originally said*, CNN (June 24, 2015).[1] The data breach, which had started in March 2014 or earlier, went on for more than a year before OPM detected it. *See*, *e.g.*, *id.*; Auerbach, David, *The OPM Breach Is a Catastrophe*, Slate (June 16, 2015).[2] Federal officials have described the OPM breach as among the largest breaches of U.S. government data in history. *Id.*

The hack was worse than the government initially believed. When OPM first disclosed the breach, it estimated that the records taken pertained to up to four million people. Further, OPM initially

---

[1] Available at http://edition.cnn.com/2015/06/22/politics/opm-hack-18-milliion/index.html.

[2] Available at http://www.slate.com/articles/technology/future_tense/2015/06/opm_hack_it_s_a_catastrophe_here_s_how_the_government_can_stop_the_next.html.

knew that sensitive information, such as Social Security numbers, names, addresses, and dates and places of birth, potentially had been compromised. *E.g.*, Risen, Tom, *China Suspected in Theft of Federal Employee Records*, US News & World Report (June 5, 2015); Sanders, Sam, *"Massive Data Breach Puts 4 Million Federal Employees' Records At Risk*, NPR (June 4, 2015). However, upon inspection, OPM determined that the breach also likely involved theft of detailed security-clearance-related background information.

Less than a month later, the government's estimate of the number of stolen records had soared to 21.5 million. This included records of people who had undergone background checks, but who were not necessarily current or former government employees. Zengerle, Patricia and Cassella, Megan, *Estimate of Americans hit by government personnel data hack skyrockets*, Reuters (July 9, 2015).

On August 27, 2017, the FBI arrested a Chinese national suspected of helping to create the malware used in the breach. Perez, Evan, *FBI arrests Chinese national connected to malware used in OPM data breach*, CNN (Aug. 28, 2017). But now, more than three years later, the damage has been done.

As a result, the past four years have seen increasing resources and focus placed on cybersecurity both in the government and the private sector. Increasingly, the term "cyberwar" is being used to describe the conflicts that loom on the horizon of digital space. Some believe we are already there. If that is so, this will be a battle waged not with guns, but keyboards. It will be fought not by soldiers, but by information security professionals, public and private.

However, this problem has emerged over time and caught many unprepared. Although the concerted efforts of stakeholders, increasing public/private collaboration, and growing awareness of these issues has led to rapid progress, the solutions are decentralized, and the growing body of law related to cybersecurity is a patchwork of new statutes and old laws stretched to apply to changing circumstances.

Information security workers on the front-lines are often the best source of identifying problems and fixes. The stakes are too high; they must be able to report concerns without fear of retaliation, lest individual managers' selfish motivations allow the next big breach.

This article, therefore, is aimed at educating information security professionals and their representatives about their legal obligations and rights. It is not comprehensive – as this broad subject could (and has) filled volumes. Rather, the goal is to survey the legal landscape to better enable cybersecurity workers to report and fix problems without fear of retaliation for exposing management's failures. We will first review some key sources of important cybersecurity regulation. The article then identifies anti-retaliation laws that could potentially protect cybersecurity professionals. Finally, we will briefly analyze how these laws could help cybersecurity whistleblowers.

II. A Survey of Federal Cybersecurity Regulation

The Executive Branch of the federal government has developed a growing interest in cybersecurity for almost a decade. While some agencies take a broader leadership role in securing the federal government's data, others focus on regulating the private sector for the public's protection.

A. Efforts to Secure Federal Systems and Assist the Private Sector

In January 2008, Pres. George W. Bush launched the Comprehensive National Cybersecurity Initiative ("CNCI"). National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23). Pres. Barack Obama then determined that the CNCI and its associated activities should become key elements of a broader, updated national U.S. cybersecurity strategy. Whitehouse Archives, The Comprehensive National Cybersecurity Initiative, available at https://obamawhitehouse.archives.gov/node/233086.

Shortly after taking office, Pres. Barack Obama ordered a comprehensive review of the federal government's cybersecurity measures. Whitehouse Archives, The Comprehensive National Cybersecurity Initiative, available at https://obamawhitehouse.archives.gov/node/233086. Pres. Obama further ordered the development of a comprehensive approach to securing America's digital infrastructure. *Id.* The resulting Cyberspace Policy Review proposed recommendations for improving the government's cybersecurity preparedness, which Pres. Obama accepted in May 2009. *Id.* Those recommendations included the selection of an Executive Branch Cybersecurity Coordinator; working closely with all key players in U.S. cybersecurity, including state and local governments and the private

sector; investing in research and development in cybersecurity; and promoting cybersecurity awareness and digital literacy. *Id.*

Pres. Donald Trump has continued to strengthen those efforts. On May 11, 2017, Pres. Trump issued Executive Order 13800 that addressed improvements for the cybersecurity of federal networks, critical infrastructure, and the nation generally. EO 13800. Though the order generally received praise from cybersecurity experts, the administration's implementation of the order has come under fire. *See* Newman, Lily, *Taking Stock of Trump's Cybersecurity Executive Order So Far*, Wired (Sept. 3, 2017).[3] However, some organizations – such as the American Civil Liberties Union – have praised Pres. Trump's actions regarding cybersecurity. Price, Greg, *Trump is Better than Obama on Cybersecurity Rules, ACLU says*, Newsweek (Nov. 28, 2017).[4] In December 2017, Pres. Trump signed into a law legislation funding national defense. The legislation included the Modernizing Government Act, a key component of the administration's effort to update the government's information technology capabilities. *See* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, M-18-12, MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES (2018). The funding is intended to "improve service delivery to the public, secure sensitive systems and data, and save taxpayer dollars." *Id.*

All federal agencies have some responsibility for cybersecurity. However, three agencies – the U.S. Department of Homeland Security ("DHS"), the Office of Budget and Management ("OMB"), and the U.S. Department of Defense ("DOD") – have far-ranging duties in securing the federal government's sensitive data. Among these leading agencies, DHS may be the most prominent.

In 2014, Congress passed the Federal Information Security Modernization Act ("FISMA") to update the federal government's cybersecurity. The statute codified DHS' authority to administer the implementation of information security policies for non-national security federal executive branch

---

[3] Available at https://www.wired.com/story/trump-cybersecurity-executive-order/.

[4] Available at http://www.newsweek.com/trump-obama-better-cybersecurity-723621.

systems, including providing technical assistance and deploying technologies to such systems.[5] *See*, *e.g.*, DHS Web site, Securing Federal Networks, available at https://www.dhs.gov/topic/securing-federal-networks. Further, FISMA clarified OMB's oversight authority over federal information security. *Id*. Additionally, FISMA obligated OMB to streamline cybersecurity reporting to avoid waste. *Id.*

As part of its expanded role, DHS' Network Security Deployment division has developed and maintains the National Cybersecurity Protection System. *Id*. The system provides intrusion detection, advanced analytics, information sharing, and intrusion prevention capabilities that combat and mitigate cyber threats to the federal government. *Id.* The National Cybersecurity Protection System is actually an integrated system of systems providing DHS a technological foundation to secure and defend the federal civilian government's information technology infrastructure.

One of the system's primary technologies is called EINSTEIN. *See*, *e.g.*, DHS Web site, Securing Federal Networks, available at https://www.dhs.gov/topic/securing-federal-networks. The EINSTEIN system detects and blocks cyber-attacks and provides DHS with situation awareness to use threat information detected in one agency to protect the rest of the government and the private sector. *Id.* DHS also operates the Continuous Diagnostics and Mitigation program that provides federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. *See*, *e.g.*, DHS Web site, Securing Federal Networks, available at https://www.dhs.gov/topic/securing-federal-networks. Additionally, DHS maintains the free Automated Indicator Sharing ("AIS") system designed to facilitate collaboration between the federal government and the private sector. *Id*. The system aims to allow instantaneous communication between companies and the federal government when an entity observes an attempted attack. *Id.* When one partner entity detects an attempted breach, all participants in the system receive immediate notification to help prevent

[5] DOD is largely responsible for implementing cybersecurity for national security systems. EO 13800.

recurrences. *Id.* The AIS may not resolve sophisticated cyber threats, but it should help shut down less-nuanced attacks. *Id.* The AIS is a result of the Cybersecurity Information Sharing Act of 2015. *Id.*

B. Federal Regulation of Private Sector Cybersecurity

1. The U.S. Securities and Exchange Commission as Cybersecurity Regulator

The U.S. Securities and Exchange Commission ("SEC") primarily regulates securities. However, in recent years, the SEC has become a leader in regulating the cybersecurity of publicly-traded corporations. It has done so primarily through applying existing regulations to address cybersecurity concerns.

a. Safeguards Rule

In an example of adapting existing rules to changing circumstances, the SEC has applied the so-called "safeguards rule" to encompass cybersecurity issues. The safeguards rule is a part of Regulation S-P. 17 C.F.R. § 248.30. The rule is designed to ensure that registered broker-dealers, investment companies, and investment advisers have policies and procedures reasonably designed to protect customers' sensitive information. *Id.*

Specifically, it provides that covered entities:

> "…must adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. These written policies and procedures must be reasonably designed to:
>
> (1) Insure the security and confidentiality of customer records and information;
>
> (2) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
>
> (3) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."
>
> *Id*.

The safeguards rule also provides for the proper disposal of sensitive records. *Id.*

In late 2015, the SEC applied the safeguards rule to deficient cybersecurity protections for the first time. *E.g.*, SEC Release No. 2015-202 (Sept. 22, 2015), available at https://www.sec.gov/news/pressrelease/2015-202.html. Investment adviser R.T. Jones Capital Equities

Management settled charges that it failed to establish cybersecurity policies and procedures as required by the safeguards rule. *Id.* R.T. Jones stored sensitive information about its clients and others on its third party-hosted web server from September 2009 to July 2013, according to the SEC's order instituting a settled administrative proceeding. *Id.* The firm's web server was hacked in July 2013, exposing to theft the sensitive information of more than 100,000 people, including thousands of R.T. Jones' clients. *Id.* At the time, the firm had no written policies and procedures reasonably designed to safeguard customer information, according to the order. *Id.* Despite the breach, there was no evidence that any clients suffered financial harm because of the attack to date, and R.T. Jones took prompt remedial actions. *Id.*

The SEC's order found that R.T. Jones violated the safeguards rule, and R.T. Jones settled the charges by agreeing to be censured, pay a $75,000 penalty, and commit no further violations. R.T. Jones did not admit or deny the SEC's findings. SEC Release No. 2015-202 (Sept. 22, 2015), available at https://www.sec.gov/news/pressrelease/2015-202.html.

This particular case is instructive in several ways. The SEC took enforcement action despite the absence of actual economic harm and although the firm took prompt remedial actions to inform and protect its clients, investigate the breach, and ensure future breaches did not recur. Further, investment advisers are among the smallest businesses the SEC regulates, and with seven employees at the time, R.T. Jones was no exception.

In recent years, the SEC has made cybersecurity under the safeguards rule an examination authority.

In February 2015, the SEC released its first Cybersecurity Examination Initiative ("CEI") examination report. OCIE, National Exam Program, *Risk Alert: Observations from Cybersecurity Examinations* (Sept. 15, 2015), available at https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf. Under the initiative, the SEC examined 57 registered broker-dealers and 49 registered investment advisers to better understand how broker-dealers and advisers address the legal, regulatory, and compliance issues associated with cybersecurity. *Id.* The SEC's Office of Compliance Inspections and Examinations ("OCIE"), which conducted the examinations, found that

almost all the examined firms had policies in place and most of the firms had experienced a cybersecurity incident. *See id.* However, the report declined to draw any conclusions about the findings. *Id.*

Ultimately, the SEC reiterated its view that the cybersecurity of registered investment companies and investment advisers is an important issue. OCIE, National Exam Program, *Risk Alert: Observations from Cybersecurity Examinations* (Sept. 15, 2015). And the SEC cited several factors, including the February 2015 report, in stressing the need for firms to review their cybersecurity measures. *Id.* In April 2015, the SEC released cybersecurity guidance outlining recommendations for effective policies and procedures. *Id.*

In August 2017, the agency released its second CEI examination report. OCIE, National Exam Program, *Risk Alert: Observations from Cybersecurity Examinations* (Aug. 7, 2017), available at https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf. This time, OCIE examined 75 covered entities for written policies and procedures regarding cybersecurity, with an increased focus on validating and testing to ensure firms were in fact implementing and following the measures. *Id.* Overall, the SEC found an improvement from its previous report but again identified concerns and recommended improvements to cybersecurity preparedness. *Id.*

b. Existing Regulation of Publicly-Traded Corporations Evolves to Include Cybersecurity

A public company may address cybersecurity issues in its public filings pursuant to its requirement to disclose significant risks to its business. If in doing so the company omits known, actual threats, it may violate the securities laws. *See Matrixx Initiatives, Inc. v. Siracusano*, 131 S.Ct. 1309 (2011). For example, investors alleged that pharmaceutical company Matrixx Initiatives, Inc. committed securities fraud by failing to disclose reports of a possible link between cold remedy Zicam (Matrixx's leading product) and loss of smell. *Id.* Investors claimed Matrixx told the market that its revenues were going to rise 50 and then 80 percent. *Id.* However, Matrixx had information indicating a significant risk to its leading revenue-generating product, according to the lawsuit. *Id.* The U.S. Supreme Court ruled

that the investors' case could proceed, reasoning that when a corporation makes a statement to the market, Rule 10b-5 requires the corporation to ensure its statements are not misleading considering all the circumstances. *Id.* Similarly, a corporation could violate the law by disclosing general cybersecurity risks pursuant to Item 503 while withholding material information about known, actual risks.

Regulation S-K prescribes certain disclosures that a corporation must include in its public filings, such as its annual report (10-K) and its quarterly report (10-Q). 17 C.F.R. Part 229. Item 503(c) of SEC Regulation S-K requires a corporation to disclose risk factors and discuss the most significant factors that make an offering speculative or risky. 17 C.F.R. Part 229.503(c). This includes the risk of cyber incidents if these issues are among the most significant factors that make an investment in the company speculative or risky. Division of Corporation Finance, U.S. Securities & Exchange Commission, CF Disclosure guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011).

A company may violate SEC Rule 10b-5 when making public disclosures if it misstates or omits a material fact. *See* 17 C.F.R. § 240.10b-5. In relevant part, the rule states:

> "It shall be unlawful for any person … [t]o make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading…in connection with the purchase or sale of any security."
>
> *Id.*

Shareholders or the SEC can bring actions against corporations that violate this rule. To do so, the SEC must prove that the corporation: 1) made a material, 2) misrepresentation and/or omission, 3) in connection with the purchase or sale of securities, and 4) the corporation had scienter. In addition to the foregoing, shareholders must also show: 1) reliance, 2) loss causation, and 3) damages. *See, e.g.*, *Halliburton Co. v. Erica P. John Fund, Inc.*, 134 S.Ct. 2398, 2407 (2014).

Hundreds of corporations disclose generalized cybersecurity risks in their public filings. If they do so while failing to disclose known actual risks, such as knowledge of an actual breach, the omission can give rise to a Rule 10b-5 action. *See Matrixx Initiatives, Inc. v. Siracusano*, 131 S.Ct. 1309 (2011).

c. February 2018 Guidance on Cybersecurity Disclosures

On February 21, 2018, the SEC took this evolution a significant step farther when it released interpretive guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents (Febraury 2018 Guidance).[6] For example, the SEC recommends that companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion. In particular, the SEC set forth the following guidance to assess materiality:

> The materiality of cybersecurity risks or incidents depends upon their nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations. The materiality of cybersecurity risks and incidents also depends on the range of harm that such incidents could cause. This includes harm to a company's reputation, financial performance, and customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities.

A corporation's failure to disclose cybersecurity issues that materially affect the corporation's financial condition and operations could violate the securities laws and regulations. For example, Item 303 of Regulation S-K requires a corporation to discuss its financial condition, changes in financial condition, and results of operations. 17 C.F.R. § 229.303. Four observations about Item 303, known as Management Discussion & Analysis, are particularly relevant to our discussion:

- One of Item 303's main purposes is to provide information about the quality of, and potential variability of, a company's earnings cash flow, so that investors can ascertain the likelihood that past performance is indicative of future performance, SEC Staff, Report on Review of Disclosure Requirements of Regulation S-K 8-10 at 42 fn. 125 (December 2013).;
- Corporations must describe any known trends or uncertainties that have had or that the corporation reasonably expects will have a material impact on net sales or revenues or income, 17 C.F.R. § 229.303(a)(3);

[6] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release Nos. 33-10459; 34-82746.

- Corporations must describe any unusual or infrequent events, transactions, or significant economic changes that materially affected the amount of reported income; and
- Corporations should address events or uncertainties that could affect past or future operations, 17 C.F.R. § 229.303 (instructions).

Because predictions about the future are inherently uncertain, the law provides a safe harbor for such forward-looking statements. But if misleading statements or omissions of *fact* are included in forward-looking statements, the corporation may not be insulated. *E.g.*, *In re Harman Int'l Indus., Inc. Securities Litigation*, 791 F.3d 90 (D.C. Cir. June 23, 2015). In *Harman*, an electronics company made forward-looking statements that reflected positively on its sales outlook. However, the plaintiffs alleged the company was aware of historical facts strongly indicating that its sales prospects were less than stellar. In holding that the plaintiffs' case could proceed, the court found that the company's cautionary statements about the forward-looking information were not meaningful because they were misleading in light of the historical facts. Because the company warned of only general, unspecified risks that could affect its rosy outlook, but did not disclose actual risks that had already manifested, the safe harbor would not apply to the forward-looking statements. The court explained that a "warning that identifies a potential risk, but 'impl[ies] that no such problems were on the horizon even if a precipice was in sight,' would not meet the statutory standard for safe harbor protection." *Id.* at 102 (internal citations omitted).

Corporations often include generic disclosures in their management discussion and analysis about cybersecurity issues that could materially affect the corporation's financial condition and operations. A company's omission of facts pertaining to an actual, known risk could violate the requirements of Regulation S-K Item 303 and possibly Rule 10b-5.

The February 2018 Guidance states that Item 303 disclosures should address "the cost of ongoing cybersecurity efforts (including enhancements to existing efforts), the costs and other consequences of cybersecurity incidents, and the risks of potential cybersecurity incidents." In addition, companies should consider addressing "costs associated with cybersecurity issues, including, but not limited to, loss of

intellectual property, the immediate costs of the incident, as well as the costs associated with implementing preventative measures, maintaining insurance, responding to litigation and regulatory investigations, preparing for and complying with proposed or current legislation, engaging in remediation efforts, addressing harm to reputation, and the loss of competitive advantage that may result."

Even if a corporation makes no mention of cybersecurity in its public filings, it may violate Sections 302 and 404 of the Sarbanes-Oxley Act if it fails to disclose material weaknesses in its internal controls related to information security. Section 302 of SOX requires a corporation's CEO and CFO to personally certify the accuracy and completeness of financial reports, and they must assess and report on the effectiveness of internal controls around financial reporting. 15 U.S.C. § 7241. Section 404 of SOX requires a corporation to assess the effectiveness of its internal controls in its annual reports, and an outside auditing firm must evaluate that assessment. Material weaknesses in those internal controls must be identified. *See*, *e.g.*, 15 U.S.C. § 7213(a)(2)(A)(iii)(III).

A material weakness is a deficiency in internal controls that presents more than a slight chance that a material misstatement of the company's financial statements will not be prevented or detected on a timely basis. PCAOB Release No. 2007-005A: An Audit of Internal Control Over Financial Reporting That is Integrated with An Audit of Financial Statements, Appendix A; *see also* Financial Accounting Standards Board Statement No. 5: Accounting for Contingencies. A deficiency in internal controls arises when a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A material weakness in internal control over financial reporting may exist even when financial statements are not materially misstated. Rather, material weakness is assessed from the potential misstatement that could occur, not the amount that is actually misstated as the result of a control deficiency. PCAOB Staff Audit Practice Alert No. 11: Considerations for Audits of Internal Control Over Financial Reporting.

SOX created the Public Company Accounting Oversight Board (PCAOB) to oversee and guide outside auditors in evaluating a corporation's internal controls. 15 U.S.C. § 7211. The PCAOB specifically has addressed auditors' need to examine corporations' information technology controls as

part of their assessment of internal controls. PCAOB Release No. 2007-005A: An Audit of Internal Control Over Financial Reporting That is Integrated with An Audit of Financial Statements; PCAOB Release No. 2010-004: Identifying and Assessing Risks of Material Misstatement. In its auditing standards, the PCAOB adopted the framework issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which also addresses information technology controls.

The SEC's February 2018 Guidance explicitly identifies and discusses the link between cybersecurity and internal controls. Thus, a corporation that fails to disclose a material weakness in its information security controls may be non-compliant with SOX. Accordingly, a disclosure of a cybersecurity issue that demonstrates a material weakness in the company's internal controls may be protected.

C. The U.S. Consumer Financial Protection Agency and Federal Trade Commission as Cybersecurity Regulators

Like the SEC, the U.S. Consumer Financial Protection Bureau ("CFPB") and U.S. Federal Trade Commission ("FTC") are federal agencies that – while they do not focus on cybersecurity specifically – have become players in cybersecurity regulation. These agencies have statutory authority to enforce laws prohibiting unfair and deceptive trade practices. And like the SEC, the CFPB and FTC have taken the view that existing laws and regulations can address cybersecurity issues. *See*, *e.g.*, *In re: Dwolla, Inc.*, Administrative Proceeding File No. 2016-CFPB-0007 (C.F.P.B. Feb. 27, 2016). As with the SEC, the CFPB and FTC do not require companies to make disclosures related to their cybersecurity. However, if a company voluntarily makes a statement about cybersecurity, the statement cannot be materially misleading.

For example, in the *Dwolla* consent order, the CFPB found that the covered person publicly represented on its Web site that it took adequate information security controls. *Id.* The order finds that the covered person failed to implement adequate information security controls. Based on this, the CFPB concluded that the covered person had engaged in unfair and deceptive practices in violation of the CFPA. *Id.*

Similarly, in August 2017, the transportation company Uber Technologies, Inc., settled the FTC's charges that it engaged in deceptive trade practices with regard to a 2014 hack. FTC Release, *Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims* (Aug. 15, 2017), available at https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data. In November 2014, after reports surfaced of Uber employees improperly accessing consumer data, the company issued a statement that it had a "strict policy" restricting employees' access to sensitive rider data and that employee access would be closely monitored on an ongoing basis. *Id.*

According to the FTC's charges, Uber quickly developed an automated system for monitoring employee access to sensitive data but stopped using it less than a year later. *Id.* The FTC's complaint alleges that during the following months Uber rarely monitored internal access to personal information. *Id.*

The FTC's complaint also alleges that despite Uber's claim that data was "securely stored within our databases," Uber's security practices failed to provide reasonable security to prevent unauthorized access to consumers' personal information in databases Uber stored with a third-party cloud provider. FTC Release, *Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims* (Aug. 15, 2017), available at https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data. As a result, an intruder accessed personal information about Uber drivers in May 2014, including more than 100,000 names and driver's license numbers that Uber stored in a data store operated by Amazon Web Services. *Id.*

The FTC alleges that Uber did not take reasonable, low-cost measures that could have helped the company prevent the breach. FTC Release, *Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims* (Aug. 15, 2017), available at https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data. For example, Uber did not require engineers and programmers to use distinct access keys to access personal information stored in the cloud. *Id.* Instead, Uber allowed them to use a single key that gave them full administrative access to all

the data and did not require multi-factor authentication for accessing the data. *Id.* In addition, Uber stored sensitive consumer information, including geolocation information, in plain readable text in database back-ups stored in the cloud. *Id.*

Most recently (and perhaps most notably) the FTC has announced an investigation into the privacy practices of social media giant Facebook. FTC Release, *Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices* (March 26, 2018), available at https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection. In response to concerns about Facebook's privacy practices, the FTC's acting director said:

> "The FTC is firmly and fully committed to using all of its tools to protect the privacy of consumers. Foremost among these tools is enforcement action against companies that fail to honore their privacy promises…Accordingly, the FTC takes very seriously recent press reports raising substantial concerns about the privacy practices of Facebook. Today, the FTC is confirming that it has an open non-public investigation into these practices."

Id.

D. Federal Contractors

Companies that contract with the federal government encounter a separate set of legal requirements that affect cybersecurity.

First, the federal government may hire a contractor specifically to provide cybersecurity related services or products. Intentionally claiming payments from the government when such work is not performed in accordance with the contract can give rise to liability under the False Claims Act ("FCA"). *E.g.*, 31 U.S.C. § 3730.

The FCA was enacted during the Lincoln administration. After the U.S. Civil War, the federal government that many contractors had not met their obligations. Because of this, Congress passed the FCA to permit the federal government to recover funds paid as a result of contractor fraud.

In addition, the federal government has established extensive regulations of federal contractor requirements. Federal contracts often specify which regulations apply to the particular contract, and these

obligations may or may not be material to the contractor's performance. Those regulations include requirements that the contractor secure the government's data.

III. State Regulation of Cybersecurity

States also play an important role in establishing cybersecurity standards for firms. Forty-eight states have cybersecurity laws on the books that, at minimum require companies to disclose when a security breach occurs. However, some states go farther and establish substantive security requirements.

For example, Massachusetts prescribes minimum requirements for companies' cybersecurity procedures, as well as substantive computer system security requirements. 201 C.M.R. §§ 17.00, et seq. Likewise, in 2015 Connecticut passed a law establishing substantive cybersecurity standards. Public Act No. 15-142. Other states like, Texas and Oregon have laws that – while stopping short of prescribing specific measures – require companies to maintain reasonable cybersecurity safeguards. *E.g.*, V.T.C.A., Bus. & C. § 521.052 (Texas); O.R.S. § 646A.622 (Oregon).

Moreover, state torts could create liability for companies whose negligence or recklessness cause harm to customers. For example, at least several of the more than 200 class action lawsuits related to the 2017 Equifax data breach pleaded simple negligence as one of the causes of action. *E.g.*, *McHill v. Equifax, Inc.*, Case No. 3:17-cv-1405 (D.O. Sept. 7, 2017).

IV. Potentially Relevant Whistleblower Laws

No federal statute directly protects cybersecurity whistleblowers from retaliation. However, much like the federal government's approach to regulation, existing laws may nonetheless provide cybersecurity professionals remedy. The following section identifies certain causes of action that may protect cybersecurity whistleblowers. The section also describes what these statutes protect, and what an employee must prove to prevail on a claim.

A. Section 806 of the Sarbanes-Oxley Act

The Sarbanes-Oxley Act ("SOX") prohibits covered employers from taking adverse employment actions against a covered worker because the worker lawfully:

- Provided information, caused information to be provided, or otherwise assisted in an investigation regarding any conduct which the employee reasonably believes constitutes a violation of section 1341, 1343, 1344, or 1348, any rule or regulation of the Securities and Exchange Commission, or any provision of Federal law relating to fraud against shareholders, when the information or assistance is provided to or the investigation is conducted by:
  - A federal regulatory or law enforcement agency,
  - Any Member of Congress or any committee of Congress, or
  - A person with supervisory authority over the employee (or such other person working for the employer who has the authority to investigate, discover, or terminate misconduct), or
- Filed, caused to be filed, testified, participated in, or otherwise assisted in a proceeding filed or about to be filed (with any knowledge of the employer) relating to an alleged violation of section 1341, 1343, 1344, or 1348, any rule or regulation of the Securities and Exchange Commission, or any provision of Federal law relating to fraud against shareholders.

Thus, the Sarbanes-Oxley Act protects covered workers when they disclose certain information to certain recipients, and it also protected certain participation in investigations and proceedings. Despite this relatively simple premise, the question of whether a worker's conduct in a specific case is protected has given rise to much litigation since the law's enactment. During that time, the case law on protected activity has evolved considerably.

To prevail on a whistleblower claim under SOX, an employee must show the following: (1) he engaged in protected activity; and (2) his protected activity was a contributing factor in the employer's decisions to take adverse employment actions against him. 18 U.S.C. § 1514A(b)(2)(C).

To engage in SOX protected activity, a "complainant need only show that he or she 'reasonably believes' that the conduct complained of constitutes a violation of the laws listed in Section 1514A."

Sylvester v. Parexel International, ARB Case No. 07-123, at *11 (ARB May 25, 2011).[7] A complainant need not establish that the protected disclosure "definitively and specifically" related to one or more of the laws listed under Section 806(a). *Id.* at *14.[8] And a SOX complainant need not establish the various elements of criminal fraud (*i.e.*, that the reported conduct was "material," intentional, relied upon by shareholders, and caused a loss to shareholders). *Id*. at *17-18. Rather, SOX protects "'all good faith and reasonable reporting of fraud.'" *Id.* at *14-15, 30 (quoting 148 Cong. Rec. S7418-01, S7420). Accordingly, the inquiry is "whether the employee reported conduct that he or she reasonably believes constituted a violation of federal law." *Id.* at *15. It is irrelevant if a complainant's disclosures are made pursuant to his job duties. *See Leznick v. Nektar Therapeutics*, ALJ No. 2006-SOX-00093 (ALJ Nov. 16, 2007).

Protection attaches when the employee provides information or assistance to anyone in the company with "supervisory authority over the employee" or with authority to "investigate, discover, or terminate misconduct." 18 U.S.C. § 1514A.

Disclosures related to the concealment of significant problems with respect to a company's compliance with federal law and internal controls implicate SEC and other federal rules and are protected under SOX.[9] Note that in securities fraud cases, courts have observed that inadequacy of internal

---

[7] Several federal courts have adopted the ARB's decision in *Sylvester*. *See, e.g.*, *Lockheed Martin Corp. v. Admin. Review Bd.,* 717 F.3d 1121, 1132 n.7 (10th Cir. 2013); *Wiest v. Lynch*, 710 F.3d 121 (3d Cir. 2013) (holding that *Sylvester* is entitled to *Chevron* deference); *Leshinsky v. Telvent GIT, S.A.*, 942 F. Supp. 2d 432, 443 (S.D.N.Y. 2013); *Stewart v. Doral Fin. Corp.*, 2014 WL 661587 (D.P.R. Feb. 21, 2014).

[8] In particular, *Sylvester* overruled *Platone v. FLYi, Inc.*, ARB Case No. 04-154, 2006 WL 3246910 (Sept. 29, 2006). In *Platone*, the ARB held that, in order to be protected, an employee's communications "must relate 'definitively and specifically' to the subject matter of the particular statute under which protection is afforded." *Id.* at *8.

[9] Section 13b of the Securities Exchange Act of 1934 states (emphasis supplied):

> Every issuer . . . shall—
>
> (A) make and keep books, records, and accounts, which, in reasonable detail, *accurately and fairly reflect the transactions . . . of the issuer*; [and]
>
> (B) *devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that—*

accounting controls "are probative of scienter [defendant's intent to deceive, manipulate, or defraud] . . . and can add to the strength of a case based on other allegations." *E.g.*, *Crowell v. Ionics, Inc.*, 343 F.Supp.2d 1, 12, 20 (D. Mass. 2004) (citations omitted). Therefore, significant deficiencies in internal controls, at least when combined with other significant issues, would constitute a circumstance likely to be "viewed by the reasonable investor as having significantly altered the 'total mix' of information made available." *Basic Inc. v. Levinson*, 485 U.S. 224, 231–32 (1988). For purposes of SOX protected conduct, "shareholder fraud" encompasses a willful attempt to conceal breaches of a company's statutory duty to disclose significant and known problems with respect to compliance with federal laws and deficiencies in internal controls.

B. Anti-Retaliation Provision of the Consumer Financial Protection Act

The Consumer Financial Protection Act ("CFPA") also provides relevant protections. In pertinent part, the CFPA provides that covered entities may not terminate covered employees because the employee has provided the employer information regarding what the employee reasonably believes to be a violation "any provision of this title or any other provision of law that is subject to the jurisdiction of the Bureau, or any rule, order, standard, or prohibition prescribed by the Bureau." 12 U.S.C. § 5567.

The law applies to any person or entity who engages in offering or providing a consumer financial product or service. 12 U.S.C. § 5481. The term "consumer financial product or service" includes a wide variety of financial products or services offered or provided for use by consumers primarily for personal, family, or household purposes, and certain financial products or services that are delivered, offered, or provided in connection with a consumer financial product or service. *See* 12 U.S.C. § 5481(5), (15). Examples of these include, but are not limited to, residential mortgage origination,

---

> (i) transactions are executed in accordance with management's general or specific authorization; [and]
>
> (ii) *transactions are recorded as necessary* (I) *to permit preparation of financial statements in conformity with generally accepted accounting principles* . . . .

15 U.S.C. § 78m(b)(2)(B) (emphasis added); *see* 17 C.F.R. §§ 230.408, 240.12b-20; *see also Craftmatic Sec. Litig. v. Kraftsow*, 890 F.2d 628, 641 (3d Cir. 1989).

lending, mortgage loan modification and foreclosure relief; student loans; payday loans; and other financial services such as credit cards, money transmitting, check cashing, and related activities. *See id.*

Similarly, the CFPA protects any "covered employee," that is, any individual performing tasks related to the offering or provision of a consumer financial product or service. 12 U.S.C. § 5567(b).

The CFPA uses an analytical framework that is substantially-identical to the one used to examine SOX retaliation claims.

C. Anti-Retaliation Provisions of the False Claims Act and National Defense Authorization Act

1. The False Claims Act Section 3730(h)

As mentioned previously, the FCA prohibits fraud on the federal government. However, the FCA also protect employees who blow the whistle on what they reasonably perceive to be fraud. Due to relatively recent amendments to the anti-retaliation provision of the False Claims Act ("FCA"), courts are increasingly broadening their view of what constitutes protected activity under the FCA. In 2009, Congress passed the Fraud Enforcement and Recovery Act of 2009 ("FERA"). Before the amendment, the FCA protected only "lawful acts done by the employee on behalf of the employee or others in furtherance of [a *qui tam* action], including investigation for, initiation of, testimony for, or assistance in an action filed or to be filed under this section."

Now, the FCA protects "lawful acts done by the employee, contractor, agent or associated others in furtherance of an action under this section or other efforts to stop 1 or more violations of this subchapter." 31 U.S.C. § 3730(h)(1). And a series of recent decisions have shown the broad latitude courts are willing to give employees under the newly amended FCA. The cases demonstrate that the FCA's whistleblower retaliation provision protects:

- internal reporting of fraudulent activity to a supervisor;
- claims where the subject of the plaintiff's disclosures would not necessarily have supported a full *qui tam*;
- steps taken in furtherance of a potential or actual *qui tam* action; and

- steps taken to remedy fraudulent activity or to stop an FCA violation.

In *United States ex rel. Lee v. Northern Adult Daily Health Care Center*, No. 13-CV-4933-MKB, 2016 WL 4703653 (E.D.N.Y. Sept. 7, 2016), former employees of Northern Adult Daily Health Care Center, a day-care center for elderly and low-income people, alleged that Northern Adult retaliated against them for their complaints about several deficiencies, including Northern Adult's unsanitary handling of food, lack of training for food-service staff, provision of alcohol to registrants, failure to provide physical therapy to residents, and disparately poor treatment of Black and Latino residents. Northern Adult took several retaliatory actions against the whistleblowers, including terminating their employment, for their attempts to stop the perceived fraud. In denying Northern Adult's motion to dismiss, the court clarified that a plaintiff need not plead an FCA retaliation claim with particularity because no showing of fraud is required. *Id.* at *5–6. The FCA protects conduct including "lawful acts done by the employee . . . in furtherance of an action under the FCA," as well as "other efforts to stop one or more violations of the FCA." *Id.* at *13. Furthermore, complaining of regulatory violations may qualify as an "effort[] to stop 1 or more violations" under the 2009 amendments to the FCA. *Id.* at *14. Such efforts to stop a violation of the FCA are protected "even if the employee's actions were not necessary in furtherance of an FCA claim." *Id.* at *13 (quoting *Malanga v. N.Y.U. Langone Med. Ctr.*, No. 14-CV-9681, 2015 WL 7019819, at *2 (S.D.N.Y. Nov. 12, 2015)). And finally, temporal proximity of less than five months is sufficient to plead causation. *Id.* at *15.

In *Marbury v. Talladega College*, Andrea Marbury sued her former employer, Talladega College, under the FCA's whistleblower protection provision. *Marbury v. Talladega Coll.*, No. 1:11-cv-03251-JEO, 2014 WL 234667 (N.D. Ala. Jan. 22, 2014). Marbury alleged that Talladega terminated her employment because she opposed requests to allocate Title III funds to advertising expenses, which is an unlawful use of Title III funds. Talladega argued that Marbury did not engage in protected conduct under the FCA because she never took any concrete steps toward bringing a *qui tam* action, could not point to a specific false claim that Talladega had submitted to the government, and made only internal complaints to her supervisor rather than filing a formal grievance or initiating a *qui tam* action.

The court rejected Talladega's narrow construction of the FCA's whistleblower protection provision. Marbury's internal opposition to using Title III funds for advertising and her refusal to complete requisition forms for unauthorized uses of Title III funds, the court found, could qualify as protected whistleblowing. *See id.* at *8. The court also rejected Talladega's argument that Marbury could not be deemed to have engaged in protected conduct because she failed to show that Title III funds were misapplied. The court noted that the whistleblower-protection provision of the FCA does not require a showing that federal funds actually were expended for an unlawful purpose—after all, the whistleblower protection provision is "intended to prevent the filing of false claims and to discourage fraud." *Id.* at *10. Had the court adopted Talladega's argument, employees who stick their necks out to stop fraud would not be protected against reprisal.[10]

In *Mikhaeil v. Walgreens Inc.*, plaintiff Mervat Mikhaeil worked as a staff pharmacist at Walgreens in July 2012, and she alleged that her employment was terminated for raising concerns about potential Medicare fraud. *Mikhaeil v. Walgreens Inc.*, No. 13-14107, 2015 WL 778179 (E.D. Mich. Feb. 24, 2015). Walgreens moved for summary judgment, and, in an opinion denying the motion in part, Judge Edmunds held that the FCA's current retaliation provision "now protects two categories of conduct": lawful acts taken in furtherance of an action under the FCA, and "other efforts to stop violations of the Act, such as reporting suspected misconduct to internal supervisors." *Id.* at *7 (internal quotations and citations omitted). The "other efforts" language, the judge observed, explicitly

[10] *Marbury* is also a good illustration of how whistleblowers can use the "cat's paw" doctrine to prove causation. Using a common tactic designed to shield employers against liability for whistleblower retaliation, Talladega assigned an official who was unaware of Marbury's disclosures to make the decision whether to terminate her employment, and then argued in its motion for summary judgment that the decision to terminate Marbury's employment could not have been motivated by retaliation. Whistleblowers can surmount that tactic by using the cat's paw theory, i.e., by showing that the decision-maker followed the biased recommendation of a subordinate without independently investigating the reason or justification for the proposed adverse personnel action. In this case, the supervisor who initiated the recommendation to terminate Marbury's employment was aware of Marbury's protected conduct, and the decision-maker simply accepted that recommendation. Applying the cat's paw doctrine, the court concluded that there was sufficient evidence of causation to permit Marbury to prove to a jury that her whistleblowing motivated the decision to terminate her employment. *See Marbury*, 2014 WL 234667, at *11.

encompasses internal reporting, which therefore constitutes protected conduct. *Id.* Mikhaeil told her supervisor the specific prescription numbers that she was concerned about, she testified. And so her disclosure about potential Medicare fraud was sufficiently specific to constitute an internal report alleging fraud on the government. *Id.* at *8.

In *Young v. CHS Middle East, LLC*, a husband-and-wife team of surgical nurses, who were working at a hospital in Iraq that ran on a State Department contract, made numerous complaints that the staffing levels on the installation were leading to employees' taking on assignments for which they were neither trained nor credentialed, in violation of CHS's contract with the State Department. *Young v. CHS Middle E., LLC*, 611 Fed. App'x 130 (4th Cir. May 27, 2015). After the Youngs lodged several complaints with their supervisors, company executives, and a State Department official, CHS terminated them both. The trial court granted CHS's motion to dismiss, holding that the Youngs' complaints about staffing did not amount to contract fraud and, therefore, were not protected by the FCA. The Youngs appealed.

While the Youngs' appeal pended, the Fourth Circuit decided a key case involving FCA *qui tam* fraud claims. In *Badr v. Triple Canopy, Inc.*, the government alleged that a security contractor responsible for base security in a combat zone had knowingly hired guards who were unable to pass contractually required marksmanship tests, yet presented claims to the government for payment on those unqualified guards. *United States ex rel. Omar Badr v. Triple Canopy, Inc.*, 775 F.3d 628, 632–33 (4th Cir. 2015). The Fourth Circuit reversed the trial court's dismissal of the claim, holding that a plaintiff successfully "pleads a false claim when it alleges that the contractor, with the requisite scienter, made a request for payment under a contract and 'withheld information about its noncompliance with material contractual requirements.'" *Id.* at 636 (quoting *United States v. Sci. Applications Intern. Corp.*, 626 F.3d 1257, 1269 (D.C. Cir. 2010)).

Applying that logic in *Young*, the Fourth Circuit reasoned that "if making false implied staffing certifications to the government can constitute a False Claims Act violation, acts undertaken to, for example, investigate, stop, or bring an action regarding such false implied staffing certifications can

constitute protected activity for purposes of a retaliation claim." *Young*, 611 Fed. App'x at 133. The Fourth Circuit, therefore, reversed the trial court's dismissal of the Youngs' claim, noting that the FCA whistleblower provision, as amended, "protect[s] employees while they are collecting information about a possible fraud, before they have put all the pieces of the puzzle together." *Id.* at 132 (alteration in original) (citation omitted).

In *Ickes v. NexCare Health Systems, L.L.C.*, Joanne Ickes, a licensed physical therapist of nearly 30 years, was hired by Integrity Rehab Services ("Integrity") to provide physical therapy services at defendant South Lyon Senior Care and Rehab Center ("South Lyon") in Michigan. *Ickes v. NexCare Health Sys., L.L.C.*, No. 13-14260, 2016 WL 1275543 (E.D. Mich. Mar. 31, 2016). South Lyon received management services from defendant NexCare Health Systems, L.L.C. ("NexCare"), which was responsible for ensuring the nursing home's compliance with federal laws and regulations. Everyone who worked at South Lyon, whether employed by South Lyon, Integrity, or NexCare, was covered by NexCare's compliance program, under which employees could report violations to South Lyon's administrator.

Ickes discovered that South Lyon employees were routinely telling patients that there were no long-term beds available for them. That is because Medicare Part A covered only short-term care (i.e., up to 100 days), and it paid more than Medicaid, which covered long-term care. The practice of denying long-term beds to patients was prohibited because South Lyon's beds were "dual-certified," meaning that "once a patient was admitted to a bed, that patient could not be told that South Lyon did not have space to continue to accommodate the patient for a long-term stay." However, this practice abounded under a South Lyon administrator whose goal it was to maintain fifty percent of the beds as short-term. After consulting an elder-law attorney, Ickes met with Integrity's president and chief operating officer and reported the nursing home's unlawful practice. Ickes followed up several times with the president/COO and reported her concerns to her supervisor, the county ombudswoman, the South Lyon administrator, Integrity's HR representative, and NexCare's HR director. The unlawful practice ceased, but only for several months. Patients began telling Ickes and another physical therapist that they had been told that no

long-term beds were available. At this point, Ickes and her colleague told their patients to "push back" because long-term beds were available and it was their right to stay. The South Lyon administrator called an emergency meeting with all physical therapists, at which she irately told them not to meddle in discharge decisions. But Ickes raised her concerns again, this time in front of the other physical therapists at the meeting. The South Lyon administrator emailed the president/COO of Integrity afterward to tell her that Ickes had been insubordinate. Ickes was subsequently suspended with pay, and, when she said she would continue to inform patients of their rights, she was terminated. Ickes filed suit against NexCare and South Lyon alleging, in part, retaliation in violation of the FCA.

Defendants NexCare and South Lyon argued that Ickes did not engage in protected conduct for two reasons: (1) "violations of patient transfer and discharge rules . . . are violations of a condition of participation not payment," and (2) "Plaintiff did not have a good-faith basis for her concerns." *Id.* at *11. The court rejected the first argument, stating in relevant part that "[t]he Act protects an employee who is punished for his or her 'efforts to stop' violations of the FCA; its protection is not limited to only those employees whose complaints turn out to prove a violation of the FCA by a preponderance of the evidence." *Id.* at *12. The plaintiff's raising the long-term-beds issue with her supervisors constituted attempts to stop the nursing home from violating the FCA by improperly discharging patients once Medicare Part A ceased to cover their therapy. The court similarly rejected the defendants' second argument, finding that Ickes clearly had a good-faith basis for her concerns given that the existence of the unlawful practice was confirmed by other therapists and patients, and Ickes spoke to an elder-law attorney and her county ombudswoman to confirm that the practice was unlawful.[11]

[11] A tangential takeaway from *Ickes* is the court's logic in finding that NexCare and South Lyon were proper defendants in the suit. NexCare and South Lyon argued that they were not covered by the FCA's anti-retaliation provision because they were not the plaintiff's direct employers. The court rejected that argument, noting that "in addition to an employee's actual employer, 'the current version of the statute also covers independent contractors and other *employment-like relationships*.'" *Ickes*, 2016 WL 1275543, at *9 (quoting *Tibor v. Mich. Orthopaedic Inst.*, 72 F. Supp. 3d 750, 759 (E.D. Mich. 2014)). Ickes was a contractor of South Lyon, so the nursing home is liable for any retaliation against her for protected conduct. *Id.* at *10. And because NexCare was in charge of Ickes's and other Integrity employees' 401(k)s, health benefits, and compliance with corporate regulations, and was integrally involved in Ickes's termination, Ickes had an "employment-like relationship" with NexCare. *Id.*

2. Sections 827 and 828 of the National Defense Authorization Act

Likewise, the 2013 National Defense Authorization Act ("NDAA") contains two robust whistleblower protection provisions that apply to employees of government contractors. *See* 10 U.S.C. § 2409. These provisions, however, exclude employee disclosures that relate to an activity of any element of the intelligence community.

Section 827 of the NDAA protects employees of contractors and subcontractors of DOD and National Aeronautics and Space Administration ("NASA"), while Section 828 applies to employees of federal contractors, subcontractors, grantees of other agencies, and others employed by entities that receive federal funds. It also applies to personal services contractors working on both defense and civilian grant programs. Both provisions protect disclosures evidencing:

- gross mismanagement of a federal contract or grant;
- a gross waste of federal funds;
- an abuse of authority relating to a federal contract or grant; or
- a substantial and specific danger to public health or safety, or a violation of law, rule, or regulation related to a federal contract.

See 10 U.S.C. § 2409, National Defense Authorization Act for Fiscal Year 2013 §§ 827–828. Furthermore, disclosures are protected only if made to:

- a member of Congress or a congressional committee;
- an Inspector General;
- the Government Accountability Office ("GAO");
- a federal employee responsible for contract or grant oversight;
- management at the relevant agency;
- an authorized official of the DOJ or other law enforcement agency;
- a court or grand jury; or

- a management official or other employee of the contractor or subcontractor, who has the responsibility to investigate, discover, or address misconduct.

See 10 U.S.C. § 2409(a)(2); 41 U.S.C. § 4712(a)(2).

The burden of proof and causation standard in NDAA whistleblower cases are very favorable to employees. A complainant need only demonstrate that the protected disclosure was a contributing factor in the personnel action, which often can be met by showing knowledge and temporal proximity. Remedies include reinstatement, back pay, compensatory damages, and attorney's fees and costs. Compensatory damages are uncapped. *See* 10 U.S.C. § 2409(c)(1); 41 U.S.C. § 4712(c)(1).

An NDAA reprisal claim must be filed initially with the Office of Inspector of General ("OIG") of the agency that awarded the contract or grant about which the employee disclosed wrongdoing. The statute of limitations is three years after the date of the reprisal. The OIG will investigate the complaint and make a recommendation to the agency head, who can order the contractor to provide relief, including reinstatement, to the NDAA complainant. If the agency head fails to provide the requested relief within 210 days, the whistleblower may bring an action in federal district court and try the case before a jury.

Section 827 of the NDAA is a permanent amendment to 10 U.S.C. § 2409, which previously provided far narrower protections to employees of DoD contractors and did not protect internal disclosures.

Section 828 was a pilot program set to expire on January 2, 2017. On December 5, 2016, Congress enacted S. 795, which made Section 828 permanent and expanded protected whistleblowers include subgrantees and personal services contractors for both defense and civilian contractors.

The enactment of the 2013 NDAA has resulted in a substantial increase in whistleblower retaliation complaints brought by employees of government contractors. Prior to August 2013, the DoD averaged just four to six whistleblower complaints per month. After the 2013 NDAA went into effect,

those numbers jumped considerably. Between January and July 2014, more than 200 whistleblower complaints were filed.[12]

D. The Whistleblower Protection Act

The Whistleblower Protection Act ("WPA") is the general catchall anti-retaliation law for employees of the federal government. 5 U.S.C. § 2302(b)(8). The WPA protects:

> "(A)any disclosure of information by an employee or applicant which the employee or applicant reasonably believes evidences—
> (i)
> any violation of any law, rule, or regulation, or
> (ii)
> gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety,
> if such disclosure is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs; or
> (B)any disclosure to the Special Counsel, or to the Inspector General of an agency or another employee designated by the head of the agency to receive such disclosures, of information which the employee or applicant reasonably believes evidences—
> (i)
> any violation (other than a violation of this section) of any law, rule, or regulation, or
> (ii)
> gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety…"
>
> *Id.*

The categories for protected activity have distinct standards, but the concepts are straightforward. For example, an employee discloses an abuse of authority when he alleges that a federal official has arbitrarily or capriciously exercised power which has adversely affected the rights of any person or has resulted in personal gain or advantage to himself or to preferred other persons, *see McCollum v. Department of Veterans Affairs,* 75 M.S.P.R. 449, 455–56 (1997), and an employee discloses a gross waste of funds when he alleges that a more than debatable expenditure is significantly out of proportion to the benefit reasonably expected to accrue to the government, *see Embree v. Department of the Treasury,* 70 M.S.P.R. 79, 85 (1996).

[12] *See* Jill Aitoro, *New Law Drove Whistleblower Complaints Against DOD Contractors Up*, WASH. BUS. J., (July 21, 2014), http://www.bizjournals.com/washington/blog/fedbiz_daily/2014/07/new-law-drove-whistleblower-complaints-against.html.

When the WPA reformers substituted "any disclosure" for "a disclosure" in the statute, they intended the small change to signify their intent to protect *all* disclosures. Congress stated explicitly it was reacting to its perception that OSC, the Board and the courts had been erecting technical barriers to exclude certain disclosures from protection. S. Rep. No. 100-143, 100th Cong., 2d Sess. 13 (1988). So, the drafters added the word "any" to modify "disclosure" to, in their words, "stress that any disclosure is protected (if it meets the requisite reasonable belief test and is not required to be kept confidential)." *Id.*

Thus, a whistleblower may disclose information to "any" person. The statute does not require that the whistleblowing occur through a specific channel (e.g., Office of Inspector General or OSC) unless the information concerns matters required by law or Presidential order to be kept confidential. 5 U.S.C. § 2302(b)(8)(A). "[I]t is inappropriate for disclosures to be protected only if they are made . . . to certain employees or only if the employee is the first to raise the issue." S. Rep. No. 413, 100th Cong., 2d Sess. 13 (1988). Section 101 of the WPEA clarified that a disclosure does not lose protection because it was made to a supervisor or other person who participated in the wrongdoing. *See Braga v. Dep't of the Army*, 54 M.S.P.R. 392, 397-98 (1992), *aff'd*, 6 F.3d 787 (Fed. Cir. 1993) (Table) (protecting memo to supervisor, oral statements made in meeting with agency officials, and memo to Chairman, Joint Chiefs of Staff, assuming disclosure to be reasonably based).

The WPA follows a similar analysis to SOX and CFPA retaliation claims. An employee establishes a prima facie case by showing by a preponderance of the evidence that: (1) he or she engaged in protected activity (and/or was associated with protected activity), (2) he or she suffered an adverse personnel action, and (3) his or her protected activity was a contributing factor in the agency's decision to take the adverse personnel actions. *See Mattil v. U.S. Dep't of State*, 118 M.S.P.R. 662, 669 (Nov. 21, 2012) (citing 5 U.S.C. § 1221(e)(1)). Then, the federal employer can avoid liability only if it shows by clear and convincing evidence that it would have taken the same action absent the whistleblower's disclosure. *See id.* (citing 5 U.S.C. § 1221(e)(2)).

E. State wrongful discharge claims

Under state law, a cybersecurity whistleblower may be able to remedy retaliation through states' public-policy exception to employment at will. *See*, *e.g.*, Muhl, Charles, *The employment-at-will doctrine: three major exceptions*, Monthly Labor Review (Jan. 2001). The vast majority of states have a public-policy exception. *See id* at 4.

Under these state causes of action, an employee is wrongfully discharged when the termination is against an explicit, well-established public policy of the state. *Id.* at 4-5. For example, in most states, an employer cannot terminate an employee for filing a workers' compensation claim after being injured on the job, or for refusing to break the law at the request of the employer. *Id.* Further, public policy derived from a state constitution, statute, or administrative rule will typically support a wrongful discharge claim. *Id.*

However, some states have either restricted or expanded the doctrine beyond these sources of policy. *Id.* For example, some courts have found that a policy was public only if it was clearly enunciated in a state's constitution or statutes and others finding that a public policy could be inferred from a statute even where the statute neither required nor permitted an employee to act in a manner that subsequently resulted in the employee's termination. *Id.*

In conclusion, though the definition of public policy varies from state to state, most states either narrowly limit the definition to clear statements in their constitution or statutes, or permit a broader definition that enables judges to infer or declare a state's public policy beyond the state's constitution or statutes.

F. Torts

As mentioned above, the public-policy exception is not the only potentially relevant state cause of action. When a company's negligent or reckless cybersecurity causes harm, they may face exposure to tort liability. Though these claims may not remedy retaliation per se, they may provide a remedy if whistleblowers separately suffer damages as the result of a breach.

V. Applying Existing Anti-Retaliation Provisions to Cybersecurity Disclosures

Though no specific anti-retaliation statute protects employees who report cybersecurity concerns, just as with substantive cybersecurity regulation, existing law may already provide whistleblowers a remedy.

A. Cybersecurity Issues Often Overlap with Well-Established Legal Concepts

In understanding whether an employee is protected by the law for reporting cybersecurity concerns, we must first address a fundamental threshold principle that has been hinted at throughout this work: issues involving information security are rarely only about information security. Cybersecurity and related terms necessarily relate to data stored (and crimes committed) electronically, on computer systems, and/or over the internet. But despite the novel technological environment, the underlying substantive issues are well trod.

The criminal case of *People v. Aleynikov* illustrates this point well. *People v. Aleynikov*, No. 1956, 2017 WL 327278 (N.Y. App. Div. Jan. 24, 2017). In Aleynikov, the defendant was a programmer at Goldman Sachs Group Inc. The government alleged that after his employment at Goldman Sachs ended, the defendant took proprietary software code without permission. A jury convicted the defendant, but the trial judge overturned the conviction on the basis that the defendant did not take any tangible property.

However, a New York state appeals court reinstated the conviction. The court noted that Goldman Sachs had taken substantial security measures to protect its valuable data. The bank had physical security, legal agreements, and a dedicated information security group. This group discovered unusual activity from the defendant's work computer when reviewing reports from its monitoring systems. The defendant put thousands of proprietary files into encrypted tarballs and uploaded them to an external site. Goldman Sachs' security system was designed to block the type of external site used, but it failed in this instance. Nonetheless, the team was quickly able to identify the breach and suspected culprit despite the defendant's alleged attempts to conceal his actions, thereby likely mitigating potential harm to the company.

The court based its holding on an examination of the statutory meaning of "tangible." But for our purposes, Manhattan District Attorney Cyrus Vance summed up the case's significance well. Vance reportedly stated that "the *theft* of intellectual property is indeed a crime…regardless of the physical means used to spirt the data away from its source." (emphasis added). Despite the digital form of the stolen property and all the implicated cybersecurity issues, this was a case about corporate theft.

The term "data leakage" has a distinct significance within the information security field. But it almost always means more than that. Data leakage can be theft, it can indicate deficient internal controls, and it can evidence a breach of contract. Cybersecurity issues are ubiquitous because the digital world is ubiquitous. However, the presence of information security concerns does not deprive the conduct at issue from its significance in other contexts. It is for this reason that whistleblowers who disclose cybersecurity concerns can be protected despite the lack of a cybersecurity-specific statute.

The remainder of this section will provide a case study of how an existing whistleblower statute can protect cybersecurity whistleblowers.

B. Cybersecurity Disclosures as Protected Activity Under SOX

As noted above, SOX protects whistleblowers when they disclose what they reasonably believe to be a violation of one or more of the six enumerated categories. The "reasonable belief" standard is key to determining whether a specific disclosure is protected.

The central inquiry to determining whether any given disclosure is protected is whether the whistleblower has a reasonable belief that she is reporting a covered violation at the time she makes the disclosure. This belief must be subjectively and objectively reasonable. *E.g.*, *Van Asdale v. Int'l Game Tech.*, 577 F.3d 989, 1000-1001 (9th Cir. 2009); *Harp v. Charter Commc'ns, Inc.*, 558 F.3d 722, 723 (7th Cir. 2009); *Menendez v. Halliburton, Inc.*, ARB Nos. 09-002, -003; ALJ No. 2007-SOX-005, slip op. at 12 (ARB Sept. 13, 2011). This means that the whistleblower must know and believe that she is reporting a covered violation, and a reasonable person in the whistleblower's circumstances must be able to reach the same conclusion. *Sylvester v. Paraxel Int'l*, ARB No. 07-123, ALJ Nos. 2007-SOX-039, -042, slip op. at 14 (ARB May 25, 2011). Thus, if a whistleblower does not believe she is reporting a violation, or

if her disclosure is outlandish or baseless in light of standards like those discussed above, the disclosure will not be protected. For example, the report of a minor information security issue that could have no significant effect on the corporation's operations may not be protected.

However, it is utterly irrelevant whether the whistleblower communicates that reasonable belief to the employer or puts the employer on notice that she is engaging in protected activity. Indeed, a disclosure can be protected even if it does not mention fraud, illegal activity, or anything that could reasonably be perceived to be a violation of the six enumerated categories in SOX. *Prioleau v. Sikorsky Aircraft Corp.*, ARB Case No. 10-060 (ARB Nov. 9, 2011).

In *Prioleau*, the whistleblower disclosed information security concerns. However, at the time of the disclosure, the whistleblower made no mention of SOX or any of the enumerated categories. Rather, the whistleblower reported his concern that two company policies were in conflict regarding a program that automatically deleted e-mails. The Administrative Review Board (an administrative appellate body that reviews SOX claims) reversed an administrative law judge's decision that the whistleblower failed to engage in protected activity. The board held that the disclosures could be protected based on evidence the whistleblower introduced during litigation, which indicated he was aware his disclosures were related to SOX compliance and that his belief was objectively reasonable.

Information security professionals should contact an experienced whistleblower attorney to determine whether SOX covers the disclosures they have made.

C. The Equifax Case Study and Applying the Analysis to a Hypothetical

On September 7, 2017, Equifax (a publicly-traded global information solutions company) announced that it had suffered a breach of data belonging to as many as 143 million Americans. That is about half the country. Worse, the breached data was sensitive: names, social security numbers, birth dates, addresses, and some driver's license numbers. Even in a world where mega breaches are commonplace, this one is staggering in both scope and severity. The total impact is impossible to foresee, but it so far it has been swift and harsh for the company.

Equifax stock immediately tumbled 13%. A modest rebound followed, but the damage has been sustained so far, wiping out the past two years of growth for the company. Multiple state and federal agencies are initiating investigations. News broke that three Equifax executives sold stock after the company discovered the breach in June, but before Equifax announced the stock. The company responded that the executives had no knowledge of the breach at the time of the transactions, but the timing could not be much worse. (And right after the SEC put consideration of an insider trading rule on the backburner despite some uncertainty arising in the courts.) To add to the problem of perception – there's no indication that the sales were prescheduled under a 10b5-1 plan.

Before the end of the month, the hack claimed the jobs of Equifax's CEO, CIO, and CSO. Hundreds of class actions have been filed. Congressional testimony has already been taken.

The developing Equifax story provides an opportunity to present a hypothetical opportunity to demonstrate that legal theory. Suppose a large, publicly-traded corporation was arguably negligent with its cybersecurity controls. Perhaps the budget was anemic, or the company did not have adequate safeguards and procedures to protect customer data, or company executives violated information security protocols. Perhaps the company delayed in reporting a breach that significantly affected its business, or did not report the breach at all.

Would an employee who reported the deficient cybersecurity have any protections under the law? Though the answer will necessarily depend on the specific facts, SOX would likely provide such an employee protection from retaliation. As noted above, the Sarbanes-Oxley Act is generally understood to protect corporate whistleblowers reporting things like shareholder fraud. However, as previously noted, cybersecurity issues often involve securities law issues. This type of hypothetical provides ample opportunity to draw those connections. Failing to disclose material deficiencies in a firm's information security could violate a public corporation's duty to disclose known risks, especially if cybersecurity *is* the public corporation's business. The company may have had a duty to file an 8K, or the company may have misrepresented its information security efforts in its public filings.

But what about an employee who has information about the misconduct but did not come forward before the cybersecurity issue was disclosed? Even then, the whistleblower laws can be of assistance. The next section briefly describes those programs. Disclosing information to the SEC that significantly contributes to an existing investigation can entitle the whistleblower to an award if certain criteria are met.

VI. Whistleblower Rewards

The Dodd-Frank Act created the SEC Whistleblower Program, which provides rewards to whistleblowers who report violations of the federal securities laws to the SEC. Eligible whistleblowers are entitled to an award of between 10% and 30% of the monetary sanctions collected in actions brought by the SEC (or related actions brought by other regulatory and law enforcement authorities).

To become eligible, an individual must submit a whistleblower tip to the SEC's Office of the Whistleblower. A tip must meet several requirements to qualify for an award. *See* 17 C.F.R. §§ 240.21F-1, *et seq*. However, a key threshold is whether the SEC opens an investigation, reopens an investigation, or inquiries into different conduct as part of a current investigation because of the whistleblower's information. New information that significantly contributes to the success of an existing matter can also qualify. Another key requirement is that the SEC action must result in an order of monetary sanctions exceeding $1 million.

In practice, the program has been picking up steam. Since the inception of the whistleblower program in 2011, the SEC has awarded more than $67 million to 29 whistleblowers. In September 2014, the agency announced a more than $30 million whistleblower award, exceeding the prior highest award of more than $14 million announced in October 2013. In May 2016 alone, the SEC awarded more than $8 million, including its third highest whistleblower award.

Whistleblower rewards also exist for those reporting violations of federal commodities laws, fraud on the government, tax underpayment, and fraud affecting banks or other financial institutions.

Information security professionals can receive rewards under the SEC Whistleblower Program and the other whistleblower rewards laws. As discussed above, cybersecurity issues and how

corporations deal with them can constitute violations of federal securities laws. And it is a good time to be an information security whistleblower. As discussed previously, the SEC has had a particular focus on cybersecurity for the past few years. As the SEC continues to address the impact to U.S. capital markets and public corporations' responsibilities to shareholders under the law, this emerging and important topic will likely remain an enforcement focus for the foreseeable future.

Similarly, whistleblowers can also recover awards for reporting fraud on the government, bank fraud and related crimes, and violations of the commodities laws.

VII. Conclusion

Cybersecurity is an issue of national prominence. To address this challenge, stakeholders should openly share information about potential threats and solutions. Though no law specifically addresses cybersecurity whistleblowing, existing laws often protect cybersecurity professionals, thereby enabling them to communicate issues without fear of retaliation.