Cybersecurity Whistleblowing:

What Employees at Public Companies Should Know Before Reporting Information Security Concerns

By Dallas Hammer – ISSA member, Quantico Chapter

No anti-retaliation statute specifically covers cybersecurity whistleblowers, but employees of public corporations may nonetheless be protected when blowing the whistle on cybersecurity concerns. This article provides a brief foundation for understanding how whistleblowers may fall within the coverage of the Sarbanes-Oxley Act of 2002 and the Dodd-Frank Act of 2010.

Abstract

No anti-retaliation statute specifically covers cybersecurity whistleblowers, but employees of public corporations may nonetheless be protected when blowing the whistle on cybersecurity concerns. The Sarbanes-Oxley Act of 2002 (SOX) prohibits retaliation against whistleblowers who disclose what they reasonably believe to be violations of the securities laws or fraud committed by publicly-traded companies. Thus, cybersecurity whistleblowers may be protected under this law if they understand when information security issues fall within the scope of the securities laws. Additionally, the Dodd-Frank Act of 2010 (DFA) may entitle whistleblowers to a monetary reward if they report a cybersecurity concern that constitutes an actual violation of the securities laws or regulations to the government. This article provides a brief foundation for understanding how cybersecurity professionals may fall within the coverage of SOX and DFA by analyzing the relationship between provisions of the securities laws and cybersecurity issues. Ultimately with some basic information and proper guidance, employees of public corporations may find that they can protect themselves when reporting cybersecurity concerns.

With cybersecurity becoming a topic of ever-increasing visibility and importance, information security professionals may ask what protection they have when they make potentially unpopular disclosures of cybersecurity issues. Though no whistleblower retaliation statute deals directly with the topic, the Sarbanes-Oxley Act of 2002 (SOX) will often protect cybersecurity professionals who work directly for public corporations or those corporations' service providers. Yet further, the Dodd-Frank Act of 2010 (DFA) could allow information security workers to receive a whistleblower reward for reporting cybersecurity concerns to the US Securities and Exchange Commission (SEC) or the US Commodity Futures Trading Commission (CFTC), in some cases.

However, the relationship among cybersecurity issues, SOX, and DFA is not yet clearly defined. Accordingly, information security professionals should educate themselves about whistleblower protections. Doing so could make the difference between being protected, receiving a whistleblower reward, or suffering retaliation without recourse.

What does SOX protect?

In relevant part, Section 806 of the Sarbanes-Oxley Act[1] forbids a covered employer to "discharge, demote, suspend, threaten, harass, or in any other manner discriminate against an employee" because of any lawful disclosure or act "regarding any conduct which the employee reasonably believes constitutes a violation of":

- Mail fraud
- Wire fraud
- Bank fraud
- Securities or commodities fraud
- Any SEC rule or regulation

1 Sarbanes Oxley Act (SOX) — 18 U.S.C. § 1514A - http://www.whistleblowers.gov/acts/sox_amended.html.

- Any provision of federal law relating to fraud against shareholders[2]

Can disclosures of cybersecurity issues be protected under SOX?

Disclosures of information security issues may be protected under SOX. As noted above, SOX protects disclosures relating to one (or more) of six categories of violations. Disclosures of cybersecurity issues can fall under that umbrella in myriad ways. I will describe just three of those scenarios.

Cybersecurity risks, Regulation SK Item 503, and SEC Rule 10b-5

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.[3]

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. Investors claimed Matrixx told the market that its revenues were going to rise 50 and then 80 percent. However, Matrixx had information indicating a significant risk to its leading revenue-generating product, according to the lawsuit. The US 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. 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).4 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.[5] 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.[6]

A company may violate SEC Rule 10b-5 when making public disclosures if it misstates or omits a material fact.[7] 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."

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 intent or knowledge of wrongdoing. In addition to the foregoing, shareholders must also show (1) reliance, (2) loss causation, and (3) damages.[8]

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.[9]

SOX in Context

Sparked by dramatic corporate and accounting scandals, the Sarbanes Oxley Act represents the most important securities legislation since the original federal securities laws of the 1930s.[1] Those scandals included those affecting Enron, Tyco International, Adelphia, Peregrine Systems, and WorldCom. Passed in 2002, SOX effected dramatic change across the corporate landscape to re-establish investor confidence in the integrity of corporate disclosures and financial reporting. President George W. Bush, who signed SOX into law, described it as "the most far-reaching reforms of American business practices since the time of Franklin D. Roosevelt. The era of low standards and false profits is over; no boardroom in America is above or beyond the law."[2] Based on the lessons learned from the corporate and accounting scandals, protecting whistleblowers formed an integral part of the reforms.[3]

1 Testimony Concerning Implementation of the Sarbanes-Oxley Act of 2002, William H. Donaldson, Chairman U.S. Securities and Exchange Commission, Before the Senate Committee on Banking, Housing and Urban Affairs – https://www.sec.gov/news/testimony/090903tswhd.htm.

2 Bumiller, Elisabeth (2002-07-31). "Bush Signs Bill Aimed at Fraud in Corporations,"*The New York Times* – http://query.nytimes.com/gst/fullpage.html?res=9C01E0D91E38F932A05754C0A9649C8B63.

3 148 CONG. REC. No. 103 (2002) (statement of Sen. Patrick Leahy) ("We learned from Sherron Watkins of Enron that these corporate insiders are the key witnesses that need to be encouraged to report fraud and help prove it in court.") – https://www.congress.gov/congressional-record/2002/7/25/senate-section/article/s7350-4?q=%7B"search"%3A%5B"%5C"We+learned+from+Sherron+Watkins+of+Enron+that+these+corporate+insiders+are+the+key+witnesses+that+%5C""%5D%7D.

2 Ibid.

3 See *Matrixx Initiatives, Inc. v. Siracusano*, 131 S.Ct. 1309 (2011) – http://www.supremecourt.gov/opinions/10pdf/09-1156.pdf.

4 17 C.F.R. Part 229 – http://162.140.57.127/cgi-bin/text-idx?SID=042a68d8eb9f43ca4bd7dc7e223d2bf7&mc=true&node=pt17.3.229&rgn=div5.

5 17 C.F.R. Part 229.503(c) – http://162.140.57.127/cgi-bin/text-idx?SID=042a68d8eb9f43ca4bd7dc7e223d2bf7&mc=true&node=se17.3.229_1503&rgn=div8.

6 Division of Corporation Finance, U.S. Securities & Exchange Commission, CF Disclosure guidance: Topic No. 2, Cybersecurity (Oct. 13, 2011) – https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

7 See 17 C.F.R. § 240.10b-5 – http://162.140.57.127/cgi-bin/text-idx?SID=042a68d8eb9f43ca4bd7dc7e223d2bf7&mc=true&node=se17.4.240_110b_65&rgn=div8.

8 See, e.g., *Halliburton Co. v. Erica P. John Fund, Inc.*, 134 S.Ct. 2398, 2407 (2014) – http://www.supremecourt.gov/opinions/13pdf/13-317_mlho.pdf.

9 See *Matrixx Initiatives, Inc. v. Siracusano*, 131 S.Ct. 1309 (2011) – http://www.supremecourt.gov/opinions/10pdf/09-1156.pdf.

Management discussion of cybersecurity issues under Regulation S-K Item 303

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. Item 303 of Regulation S-K requires a corporation to discuss its financial condition, changes in financial condition, and results of operations.[10] 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[11]
- 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[12]
- Corporations must describe any unusual or infrequent events, transactions, or significant economic changes that materially affected the amount of reported income
- Corporations should address events or uncertainties that could affect past or future operations[13]

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.[14] 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."15

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. Thus, reporting an information security issue that contradicts or undermines the company's management discussion and analysis of cybersecurity could be protected under SOX.

10 17 C.F.R. § 229.303 – http://162.140.57.127/cgi-bin/text-idx?SID=042a68d8eb9f43ca4bd7dc7e223d2bf7&mc=true&node=se17.3.229_1303&rgn=div8.

11 SEC Staff, Report on Review of Disclosure Requirements of Regulation S-K 8-10 at 42 fn. 125 (December 2013) – https://www.sec.gov/news/studies/2013/reg-sk-disclosure-requirements-review.pdf.

12 17 C.F.R. § 229.303(a)(3).

13 17 C.F.R. § 229.303 (instructions).

14 E.g., *In re Harman Int'l Indus., Inc. Securities Litigation*, 791 F.3d 90 (D.C. Cir. June 23, 2015) – https://www.cadc.uscourts.gov/internet/opinions.nsf/1B7208ADC298E6C985257E6D00539C76/$file/14-7017-1559106.pdf.

15 Ibid. at 102 (internal citations omitted).

Material weaknesses in internal controls under SOX Sections 302 and 404

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.[16] 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.[17]

16 15 U.S.C. § 7241 – http://uscode.house.gov/view.xhtml?req=(title:15 section:7241 edition:prelim) OR (granuleid:USC-prelim-title15-section7241)&f=treesort&edition=prelim&num=0&jumpTo=true.

17 See, e.g., 15 U.S.C. § 7213(a)(2)(A)(iii)(III) – http://uscode.house.gov/view.xhtml?req=(title:15 section:7213 edition:prelim) OR (granuleid:USC-prelim-title15-section7213)&f=treesort&edition=prelim&num=0&jumpTo=true.

WIS SIG: Regulatory Compliance – A Change Management Challenge

Continued from page 8

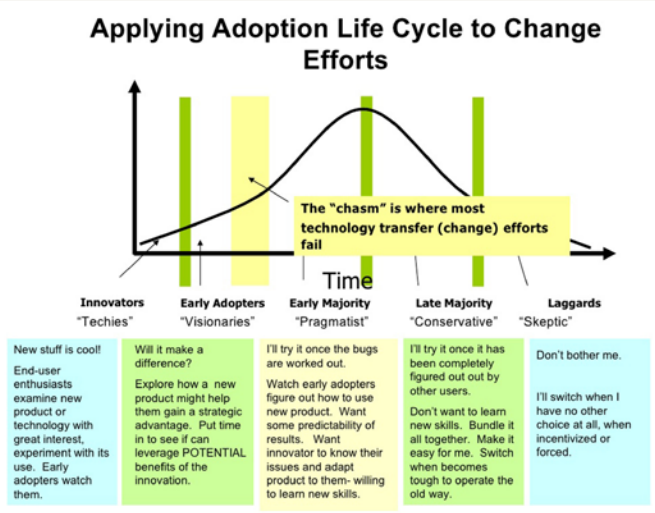

Figure 5 – Change adoption cycle

just published the ISSA's Alliance for Performance Excellence, National Institute of Standards and Technology's Baldrige Program.[1] ISSA members will have access to a free Baldrige-based self-assessment tool, named the Security Success Score,[2] which allows ISSA members to assess the performance excellence of security operations in light of NIST-based and Baldrige-based frameworks. The best of both worlds heightens cyber-resiliency and enables their dedicated practitioners and organizations to excel through the change process, raising quality and performance levels with this one cohesive program.

Figure 6 – Business excellence framework

Figure 7 depicts at a high level the core elements associated with the Baldrige framework. Armed with these new tools and new-found knowledge, we will have the opportunity to impact high levels of positive change, turning regulatory complexity and headaches into stakeholder- and organization-integrated implementation successes. Assure away SMEs!

Figure 7 – Baldrige performance excellence criteria

Join the international conversation at #ISSAWISSIG, WIS-SIG@ISSA.ORG, and via LinkedIn.

Be BRAVE, Be BOLD, Own Your Future!

About the Author

Dr. Rhonda Farrell, J.D., CISSP, CSSLP is an Associate at Booz Allen Hamilton (BAH) and a member of the Board of Directors at ISSA Intl and ISSA-NOVA. She also holds an officer position within IEEE and committee positions within ASQ. She is the Co-Founder of the WIS SIG and works cross-organizationally to actively enhance cybersecurity-oriented programs internationally. She can be reached at rhondalfarrell@aol.com.

1 Alliance for Performance Excellence and ISSA Offer Free Cyber Maturity Tool to ISSA Members, Alliance for Performance Excellence – http://www.baldrigepe.org/alliance/.

2 Managehub, Cybersecurity Success Score – https://www.managehubaccelerator.com/cybersecurity-success-score/.

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.[18] 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.[19]

SOX created the Public Company Accounting Oversight Board (PCAOB) to oversee and guide outside auditors in evaluating a corporation's internal controls.[20] The PCAOB specifically has addressed auditors' need to examine corporations' information technology controls as part of their assessment of internal controls.[21] 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.

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.

Shareholder fraud, internal controls, and SOX

For the reasons described above, an information security professional's disclosure of a public corporation's cybersecurity issues can be protected under SOX. A corporation failing to disclose information security issues could be committing shareholder fraud or violating SEC rules relating to internal controls. However, these scenarios are far from exhaustive. SOX could protect the reporting of cybersecurity issues under many circumstances.

When is a specific disclosure protected?

Though cybersecurity whistleblowers can make SOX-protected disclosures, such protection is not automatic. 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.[22] 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.[23] 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.[24]

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 emails. 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.

Other protections may also apply

In addition to SOX, numerous other laws may cover cybersecurity workers who blow the whistle, but like SOX may or may not apply depending on the specific facts. For example, if an information security issue constitutes misconduct re-

18 PCAOB Release No. 2007-005A: An Audit of Internal Control Over Financial Reporting That is Integrated with An Audit of Financial Statements, Appendix A – http://pcaobus.org/Rules/Rulemaking/Docket 021/2007-06-12_Release_No_2007-005A.pdf; see also Financial Accounting Standards Board Statement No. 5: Accounting for Contingencies – http://www.fasb.org/jsp/FASB/Document_C/DocumentPage?cid=1218220126761&acceptedDisclaimer=true.

19 PCAOB Staff Audit Practice Alert No. 11: Considerations for Audits of Internal Control Over Financial Reporting – http://pcaobus.org/standards/qanda/10-24-2013_sapa_11.pdf.

20 15 U.S.C. § 7211 – http://uscode.house.gov/view.xhtml?req=15+usc+7211&f=treesort&fq=true&num=9&hl=true&edition=prelim&granuleId=USC-prelim-title15-section7211.

21 PCAOB Release No. 2007-005A: An Audit of Internal Control Over Financial Reporting That is Integrated with An Audit of Financial Statements –http://pcaobus.org/Rules/Rulemaking/Docket 021/2007-06-12_Release_No_2007-005A.pdf; PCAOB Release No. 2010-004: Identifying and Assessing Risks of Material Misstatement – http://pcaobus.org/Rules/Rulemaking/Docket 026/Release_2010-004_Risk_Assessment.pdf.

22 E.g., *Van Asdale v. Int'l Game Tech.*, 577 F.3d 989, 1000-1001 (9th Cir. 2009) – https://cdn.ca9.uscourts.gov/datastore/opinions/2009/08/13/07-16597.pdf; *Harp v. Charter Commc'ns, Inc.*, 558 F.3d 722, 723 (7th Cir. 2009) – http://media.ca7.uscourts.gov/cgi-bin/rssExec.pl?Submit=Display&Path=Y2009/D03-16/C:07-1445:J:Rovner:aut:T:fnOp:N:225637:S:0; *Menendez v. Halliburton, Inc.*, ARB Nos. 09-002, -003; ALJ No. 2007-SOX-005, slip op. at 12 (ARB Sept. 13, 2011) – http://www.oalj.dol.gov/PUBLIC/ARB/DECISIONS/ARB_DECISIONS/SOX/09_002.SOXP.PDF.

23 *Sylvester v. Paraxel Int'l,* ARB No. 07-123, ALJ Nos. 2007-SOX-039, -042, slip op. at 14 (ARB May 25, 2011) – http://www.oalj.dol.gov/PUBLIC/ARB/DECISIONS/ARB_DECISIONS/SOX/07_123.SOXP.PDF.

24 *Prioleau v. Sikorsky Aircraft Corp.*, ARB Case No. 10-060 (ARB Nov. 9, 2011) – http://www.oalj.dol.gov/PUBLIC/ARB/DECISIONS/ARB_DECISIONS/SOX/10_060.SOXP.PDF.

SURVIVAL STRATEGIES IN A CYBER WORLD

Hyatt Regency | **NOVEMBER 2-3** | Dallas, Texas

PREDICT PREPARE PROTECT

ISSA International CONFERENCE

2016

REGISTER TODAY

EARLY BIRD RATES

UNTIL JUNE 30

DETAILED PROGRAM HERE

NOVEMBER 2-3, 2016

HYATT REGENCY | DALLAS, TEXAS

lated to a federal contract or grant, several laws may protect cybersecurity professionals from reprisal.[25] If the misconduct involves fraud on the government, the False Claims Act may provide protection from retaliation, as well as an opportunity for a whistleblower reward.[26] Similarly, federal employees who report an information security issue they believe constitutes a violation of law, rule, or regulation or other specified misconduct may be covered by the Whistleblower Protection Act.[27]

In short, though no specific law protects cybersecurity whistleblowers, many anti-retaliation laws may nonetheless protect information security workers who report problems. However, the patchwork of provisions requires careful analysis to determine which laws could apply to any given real-world scenario.

How can cybersecurity whistleblowers receive a reward?

The Dodd-Frank Act created the SEC Whistleblower Program,[28] 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.[29] However, a key threshold is whether the SEC opens an investigation, reopens an investigation, or inquires 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,[30] exceeding the prior highest award of more than $14 million[31] announced in October 2013. In May 2016 alone, the SEC awarded more than $8 million,[32] 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 I have discussed in a previous article,[33] the SEC has had a particular focus on cybersecurity for the past few years. As the SEC continues to address the impact to US 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.

Key Considerations for Obtaining an SEC Whistleblower Reward

- A whistleblower must voluntarily give the SEC original information about a possible violation of the federal securities laws that has occurred, is ongoing, or is about to occur.
- More than one person can act together as whistleblowers, but companies and organizations do not qualify.
- A whistleblower need not be a current or former employee to be an eligible whistleblower.
- Whistleblowers who are represented by attorneys can remain anonymous when reporting through the SEC Whistleblower program.
- Cybersecurity professionals can be eligible for awards by providing independent analysis regarding violations of federal securities laws, even if they have no employment relationship with the company.
- Other exclusions and limitations may apply.[1]

You can find out more about the SEC Whistleblower Program here.

1 See 17 C.F.R. §§ 240.21F-1, et seq – https://www.sec.gov/about/offices/owb/reg-21f.pdf - nameddest=21F-2.

Conclusion

As the foregoing illustrates, there are many circumstances where blowing the whistle on cybersecurity issues related to a

25 E.g., 41 U.S.C. § 4712; 10 U.S.C. § 2409 – http://uscode.house.gov/view.xhtml?req=(title:10 section:2409 edition:prelim) OR (granuleid:USC-prelim-title10-section2409)&f=treesort&edition=prelim&num=0&jumpTo=true.

26 See 31 U.S.C. § 3730 (a whistleblower reward claim under the False Claims Act is known as a qui tam action and differs significantly from most other whistleblower rewards statutes) – http://uscode.house.gov/view.xhtml?req=(title:31 section:3730 edition:prelim) OR (granuleid:USC-prelim-title31-section3730)&f=treesort&edition=prelim&num=0&jumpTo=true.

27 5 U.S.C. § 2302(b)(8) – http://uscode.house.gov/view.xhtml?req=(title:5 section:2302 edition:prelim) OR (granuleid:USC-prelim-title5-section2302)&f=treesort&edition=prelim&num=0&jumpTo=true.

28 Office of the Whistleblower, SEC – https://www.sec.gov/whistleblower.

29 See 17 C.F.R. §§ 240.21F-1, et seq – https://www.sec.gov/about/offices/owb/reg-21f.pdf - nameddest=21F-2.

30 SEC Announces Largest-Ever Whistleblower Award – https://www.sec.gov/News/PressRelease/Detail/PressRelease/1370543011290.

31 SEC Awards More Than $14 Million to Whistleblower – https://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539854258.

32 SEC Awards More Than $5 Million to Whistleblower – https://www.sec.gov/news/pressrelease/2016-91.html.

33 SEC Enforcement Action Portends Rewards for Cybersecurity Whistleblowers – https://www.zuckermanlaw.com/sec-enforcement-action-portends-rewards-for-cybersecurity-whistleblowers/.

public company could be protected under the law, despite the lack of a whistleblower retaliation law aimed directly at cybersecurity whistleblowers. Further, cybersecurity issues may entitle whistleblowers to an award if they report actual violations of the securities laws to the SEC. However, ensuring such protection requires an understanding of how cybersecurity issues at public companies relate to the securities laws and rules regulating those companies.

About the Author

Dallas Hammer is an attorney at Zuckerman Law and chairs the firm's Whistleblower Rewards Practice Group. Mr. Hammer's practice largely focuses on representing corporate and financial institution whistleblowers before federal agencies such as the Securities Exchange Commission, Department of Justice, and Department of Labor. He may be reached at dhammer@zuckermanlaw.com.

"THE TREE OF LIBERTY MUST BE REFRESHED FROM TIME TO TIME WITH THE BLOOD OF PATRIOTS AND TYRANTS."

— Thomas Jefferson, Paris, November 13, 1787

So, too, must our code of ethics be revisited from time to time by those who abide by it and who vow to uphold it.

ISSA Code of Ethics

The primary goal of the Information Systems Security Association is to promote practices that will ensure the confidentiality, integrity, and availability of organizational information resources. To achieve this goal, members of this Association must reflect the highest standards of ethical conduct. Therefore, ISSA has established the following Code of Ethics and requires its observance as a prerequisite for continued membership and affiliation with the Association.

As an ISSA member, guest, and/or applicant for membership, I have in the past and will in the future:

- Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles;
- Promote generally accepted information security current best practices and standards;
- Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities;
- Discharge professional responsibilities with diligence and honesty;
- Refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation of or is detrimental to employers, the information security profession, or the Association; and
- Not intentionally injure or impugn the professional reputation or practice of colleagues, clients, or employers.