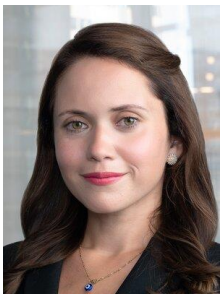
Twitter Whistleblower Claim Is Cautionary Tale For Employers

By **Gregory Keating, Brian Cesaratto and Ashley Krezmien** (September 28, 2022)

Gregory Keating

Brian Cesaratto



Ashley Krezmien

The widely reported recent whistleblower complaint by Twitter Inc.'s former chief of security Peiter Zatko highlights the importance of employers having policies and procedures in place to effectively address concerns repeatedly raised by cybersecurity professionals.

The whistleblower complaint[1] and its continuing fallout, including Zatko's testimony[2] before Congress, reveal how the triad of cybersecurity obligations to safeguard data, cyber incident reporting rules and whistleblower protections can result in litigation, regulatory activity and reputational harm when cyber professionals' repeated concerns are not addressed to their satisfaction.

The dueling press statements on behalf of Zatko and his employer offering up competing accounts should serve as the proverbial wake-up call for organizations employing cybersecurity professionals to quickly and effectively respond when repeated internal concerns over security practices are raised.

To avoid whistleblower litigation and regulatory scrutiny, while complying with their cybersecurity obligations, employers should develop written protocols that anticipate the inevitable raising of cybersecurity concerns by cyber professionals, including a process to escalate concerns to legal counsel or independent cyber professionals when necessary to mediate competing views.

Employers should clarify whether the employee is raising a whistleblower complaint alleging legal violations, or, rather, is acting within the scope of addressing normal concerns. Employers should also convey that concerns may be raised without the fear of retaliation.

Organizations that hold protected data — e.g., personal information, government identifiers, medical data, financial information — are subject to regulations requiring that reasonable safeguards be taken to protect that data from certain risks, e.g., a risk that a hacker will steal consumer/patient identities or sensitive information or launch a ransomware attack.

There are numerous risk management frameworks, e.g., National Institute of Standards and Technology Cybersecurity Framework,[3] HitTrust CSF,[4] ISO 27001 and 27002,[5] SANs Critical Security Controls[6] to reduce the risk of an organization suffering a damaging data breach or other cyberattack through a mix of administrative, technical and physical safeguards.

Organizations also frequently adopt written information security programs to address the particular cyber risks and potential negative impacts they face. Risk management frameworks rely on organizations hiring qualified cybersecurity professionals to secure the organization's sensitive data and systems.

Part of a cybersecurity professional's job duties is to implement reasonable safeguards based on an assessment of risk, which in many cases may be wholly or partly subjective.

As a result, as part of their normal job duties, cybersecurity professionals critique, opine on and openly disagree about the level of risk involved and the safeguards that should be employed to address those risks.

An organization's capability to reduce cybersecurity risks depends on employees raising concerns as part of their everyday job duties and having those concerns addressed as part of the organization's adoption of a risk management framework or internal information security program, e.g., NIST Cybersecurity Framework — governance,[7] risk assessment, risk management strategy.[8]

At the same time, there are laws requiring notification of data breaches. There are also increasingly actual or proposed requirements mandating that certain cyber risks and incidents — such as ransomware attacks — that may not result in a data breach be reported by organizations to government regulators.

In the wake of certain well publicized cyberattacks — e.g., Solar Winds, Colonial Pipeline — there is a clear trend toward greater transparency as to cybersecurity decision-making, particularly where a successful attack may affect critical infrastructure and national interests.

On Feb. 9, for example, the U.S. Securities and Exchange Commission proposed rules[9] requiring registered investment advisers and funds to adopt and implement written policies and procedures to reasonably address cybersecurity risks and report on their cybersecurity risk determinations and significant cybersecurity incidents.

On March 9, the SEC proposed rules[10] requiring reporting on policies and procedures to manage cybersecurity risks, management's role in implementing those policies and procedures, level of board's cybersecurity expertise and oversight of cyber risks, and updates on previously reported material cybersecurity incidents.

On March 15, President Joe Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022,[11] requiring reporting — upon completion of rulemaking — by critical infrastructure organizations of certain cyber incidents, e.g., payments made pursuant to a ransomware attack.

This regulatory trend is likely to continue and will result in greater transparency into the day-to-day judgments cyber professionals make as part of their job duties and responsibilities.

Lastly, anti-retaliation and other protections are in place for certain employees who bring violations of law to light. For example, the U.S. Department of Justice recently announced its new Civil Cyber-Fraud Initiative, promising to utilize the False Claims Act to better support qui tam whistleblowers and address cybersecurity-related fraud regarding government contracts and grant recipients.

According to the DOJ's press announcement,[12] this initiative seeks to hold accountable

> entities or individuals that [place] U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting

their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cyber security incidents and breaches.

Only months later, the DOJ announced its two first sizable settlements under the Civil Cyber-Fraud Initiative. On March 8, the DOJ announced[13] its $930,000 settlement with Comprehensive Health Services Inc. for allegations that two whistleblowers raised under the FCA's qui tam provisions.

According to the press announcement, Comprehensive Health Services failed to report that it inconsistently maintained the confidentiality of government employees' medical records, stored records on an unsecured internal network drive and ignored staff concerns about Comprehensive Health Services' unsecured storage of this protected information.

On July 8, the DOJ announced[14] a settlement under its Civil Cyber-Fraud Initiative against Aerojet Rocketdyne Holdings Inc., a federal government contractor.

The settlement followed Aerojet's former senior director of cybersecurity suing the company under the FCA's qui tam provisions, alleging that Aerojet fraudulently induced the government to contract with Aerojet by misleading the government about its compliance with cybersecurity requirements for defense contractors to protect uncontrolled unclassified information and other sensitive information.

Aerojet settled the matter on the second day of trial for $9 million, with $2.61 million falling to the employee.

The DOJ emphasized in its press announcement that "whistleblowers with inside information and technical expertise can provide crucial assistance in identifying cybersecurity failures and misconduct." Thus, employees who become frustrated have the ability to bring legal violations to the attention of the courts and regulators.

From a whistleblowing perspective, companies dealing with those tasked with identifying cyber issues face a vexing hurdle. Namely, it is often inherent in the nature of those individuals' jobs to spot and remediate problems.

Accordingly, how and when is an employer to know that the individual is engaging in protected activity by blowing the whistle?

Indeed, courts have struggled with the question of the impact of a complainant's job duties on whether the individual engaged in protected activity.[15] However, in a number of decisions over the past decade, the courts have concluded that the Sarbanes-Oxley Act, or SOX, does not place a duty speech restriction on protected activity.

Focusing on the purpose of SOX — encouraging the reporting of corporate fraud — courts and the Department of Labor have repeatedly found that the nature of the reporting employee's job duties is irrelevant.[16]

However, in Riddle v. First Tennessee Bank in 2011, the U.S. District Court for the Middle District of Tennessee declined to find protected activity where the plaintiff's reports were made entirely in his role as a corporate security investigator.[17]

In that case, the court found that, although the plaintiff reported the employee's misconduct to his supervisors, he did not step outside his role as an investigator and take additional action, which was necessary to establish protected activity.

Given — and as noted — that it can be difficult to tell whether an individual is simply doing his or her job or acting as a whistleblower, employers dealing with those in information technology and cybersecurity should be on the lookout for those who complain repeatedly regarding a problem or issue relating to cybersecurity.

If and when an individual persists in raising an issue relating to cybersecurity when it is within their job to address and remediate concerns, employers should consider escalating appropriately to in-house counsel or compliance and conducting an independent review.

Employers should contemporaneously document whether an employee is raising legal violations in the event that the employee later seeks to assert retaliation.

Employees should consult with counsel before subsequently taking any adverse action against the individual who raised the concerns.

Gregory Keating and Brian G. Cesaratto are members, and Ashley Krezmien is a law clerk, at Epstein Becker Green.

[1] https://www.washingtonpost.com/technology/interactive/2022/twitter-whistleblower-sec-spam/.

[2] https://www.judiciary.senate.gov/press/dem/releases/senate-judiciary-committee-releases-testimony-of-twitter-whistleblower-peiter-mudge-zatko.

[3] https://www.nist.gov/industry-impacts/cybersecurity-framework.

[4] https://hitrustalliance.net/product-tool/hitrust-csf/?gclid=EAIaIQobChMI8IWvrPuj-gIVFLrICh169wNBEAAYAiAAEgJ1m_D_BwE.

[5] https://www.iso.org/isoiec-27001-information-security.html.

[6] https://www.cisecurity.org/controls/cis-controls-list.

[7] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[8] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[9] https://www.workforcebulletin.com/2022/03/18/president-biden-signs-into-law-the-cyber-incident-and-reporting-act-mandating-reporting-of-cyber-incidents-and-ransomware-payments/.

[10] https://www.sec.gov/news/press-release/2022-39.

[11] https://www.workforcebulletin.com/2022/03/18/president-biden-signs-into-law-the-cyber-incident-and-reporting-act-mandating-reporting-of-cyber-incidents-and-ransomware-

payments/.

[12] https://www.subjecttoinquiry.com/2021/10/department-justice-announces-increased-fca-enforcement-through-new-civil-cyber-fraud-initiative/.

[13] https://www.justice.gov/opa/pr/medical-services-contractor-pays-930000-settle-false-claims-act-allegations-relating-medical.

[14] https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity.

[15] See, e.g., Garcetti v. Ceballos, 547 U.S. 410, 421 (2006) (holding First Amendment does not protect government employees from employer discipline for statements made pursuant to official duties); Sasse v. Department of Labor, 409 F.3d 773, 780 (6th Cir. 2005) (U.S. attorney who alleged DOJ retaliated against him while investigating environmental crimes failed to show agency violated whistleblower provisions of environmental laws because performance of his job duties was not protected whistleblowing activity); Langer v. Department of the Treasury, 265 F.3d 1259, 1266-67 (Fed. Cir. 2001) (IRS employee, whose duty it was to review actions taken by the IRS's Criminal Division, did not engage in activity protected by the WPA by informing DOJ officials that their grand jury investigations disproportionately targeted African-Americans).

[16] See, e.g., Wiest v. Lynch, 710 F. 3d 121, 129 (3d Cir. 2013) (an accountant who was performing his job duties when he raised questions about treatment of business expenses and put company on notice of possible violation of a "provision of Federal law relating to fraud against the Shareholders" had a viable SOX retaliation claim); Yang v. Navigators Grp. Inc., 18 F. Supp. 3d 519, 528 (S.D.N.Y. 2014) (holding that the fact that the plaintiff was hired to report risk issues does not mean he cannot satisfy the SOX reporting requirement), vacated on other grounds, 674 F. App'x 13 (2d Cir. 2016); Barker v. UBS AG, 888 F. Supp. 2d 291, 297 (D. Conn. 2012) (concluding that SOX "does not indicate that an employee's report or complaint about a protected violation must involve actions outside the complainant's assigned duties");.

[17] Riddle v. First Tenn. Bank, Nat'l Ass'n, No. 3:10-cv-0578, 2011 WL 4348298, at *8 (M.D. Tenn. Sept. 16, 2011), aff'd. 497 F. App'x 588, 598 (6th Cir. 2012).