Employee Threats to Critical Technologies Are Best Addressed Through a Formalized Insider Threat Risk Assessment Process and Program

By Brian G. Cesaratto and Robert J. Hudock

The pace of innovative technology in financial services and other industries is accelerating. Firms are investing heavily to develop the next cutting-edge applications that will drive future growth. Industry efforts have expanded the "attack surface" of these new technologies to dishonest employees and other malicious insiders. As the scope and criticality of these information systems increase, there is a corresponding increase in the number of employees and other insiders (e.g., a vendor or service provider's workers) who have or may seek to gain access for a financial motive or other illegitimate purposes. To best protect against insider threats, firms should develop an insider threat program comprised of workforce management policies and procedures and technical controls that specifically consider insider risks from employees and trusted business partners' workers. A formalized and targeted risk assessment process is the best way to ensure the most effective combination of personnel measures and technical controls to counter the insider risks faced by the firm and its industry.

Brian G. Cesaratto

Robert J. Hudock

"The government alleged that following a negative performance review and after being advised that he would not be receiving a compensation increase, the engineer used his work computer to download over 800 files and folders from a restricted network drive he had access to as a member of the engineering team."

By definition, "insiders" already have authorized access to a firm's systems and the information contained therein. They have been issued credentials (e.g., usernames, passwords) authorizing their electronic access. A malicious insider is a current or former employee, third party contractor or other business partner who has or had authorized access to the firm's network, systems or data and intentionally exceeds or misuses that access in a manner that negatively affects the confidentiality, integrity or availability of the firm's information or information systems. In other words, insiders are already inside the proverbial castle walls and have access to the "keys to the kingdom."

Insider risks involve different considerations than the risks posed by external hackers because of the insiders' trusted access. The risk assessment process, consequently, needs to focus internally by anticipating the actions that employees may take to exfiltrate trade secrets or otherwise do harm and the corresponding protective measures to counter the threats posed. The most effective approach for examining those threats is to treat each user or group of users not as trusted users, but as potentially malicious actors, and then design appropriate defensive strategies.

Successful strategies to counter malicious insider behavior ultimately depend heavily on personnel and legal departments working closely with their IT counterparts. Personnel policies and programs must closely support the system related controls implemented to protect against insider threats (e.g., robust workplace monitoring policies should be in place to support a data loss prevention/deep packet inspection program). Personnel departments, moreover, are often the first line of defense because they are the "eyes and ears" of the organization, and often the earliest to become aware of employee issues posing a cyber security risk to vital trade secrets (e.g., current drug or alcohol use, financial and credit troubles, disgruntlement).

For firms looking to protect their key technologies, the sophisticated methods that employees will utilize to unlawfully acquire key software and other electronically stored trade secrets is chilling. Recent cases provide representative examples of insider risks and the corresponding need for a formalized insider risk assessment program. Indeed, within the last year, in separate criminal matters, two computer engineers were arrested by federal authorities and charged with alleged attempted theft of trade secrets comprised of a proprietary computer code used to run the trading platforms of their respective financial services employers.[1] The risks posed by employee and other insider theft of employer technology in financial services and other industries is not new,[2] but the

Reprinted with permission from: *Labor and Employment Law Journal*, Spring 2018, Vol. 43, No. 1, published by the New York State Bar Association, One Elk Street, Albany, NY 12207.

stakes for firms in taking appropriate protective measures to prevent exfiltration are escalating as the technologies become ever more important to the future bottom line.

For example, in *United States v. Sazonov,*[3] the government alleged that the defendant software engineer stole critical information related to the firm's trading platform designed to analyze data and automatically implement trading strategies. The engineer allegedly logged into the firm's system and then logged into the software repository storing the platform's source code, copying the source code into a pdf file and then encrypting the file. The engineer had an additional unique log-in identifier and password to gain access to the software repository (i.e., he was a privileged user). He used steganography (which is a sophisticated method of hiding data) to conceal pieces of the source code in unencrypted form into otherwise outwardly innocuous documents and files. He allegedly exfiltrated both the encrypted and unencrypted files he had created through separate emails to an external email account he had set up under a fictitious name. He also allegedly used an "old school" method to steal the source code, printing out portions of the stolen files from his work computer and physically carrying the copies out of the office.

Similarly, the indictment of a former engineer who was part of a team working on developing cutting edge concealment fabric technology for a clothing manufacturer further highlights the sophisticated measures insiders will use to steal trade secrets. The government alleged that following a negative performance review and after being advised that he would not be receiving a compensation increase, the engineer used his work computer to download over 800 files and folders from a restricted network drive he had access to as a member of the engineering team. The engineer then allegedly transferred the files to external hard drives and other storage media he attached to his work computer, including confidential information related to the technical fabrics being developed.[4]

Firms are, therefore, well served by utilizing a formalized vulnerability and risk assessment process to identify insider threats to the confidentiality, integrity, and availability of their most critical technologies and systems and to address the specific risks. A formalized risk assessment process is a well-recognized best practice. New York State registered or licensed financial services firms are required to conduct vulnerability assessments biannually and risk assessments on a periodic basis.[5] Federal Trade Commission regulated financial institutions are also required to conduct risk assessments relevant to safeguarding non-public customer information.[6] The National Association of Insurance Commissioners has adopted a model cybersecurity law requiring a formalized risk assessment process.[7] NIST and ISO guidance also provide for periodic risk assessments.[8] An insider threat risk assessment should be part of the firm's overall risk assessment process.

In conducting an insider threat risk assessment, firms should identify their critical information systems and the supporting hardware and interconnected communication systems. The job roles associated with those key systems—i.e., any insider who by virtue of his or her job position will be granted access to trade secrets and critical data—should be identified. In particular, managerial and other roles that permit privileged access to the systems should be pinpointed (e.g., database or network administrators, super users, domain administrators, software developers). Comprehensive functional job descriptions relevant to the access to critical data and technologies should be developed detailing the interactions between the employee and the information. A map, chart, or other graphical representation of the systems and insiders should be made so that the organization can thoroughly understand the interconnectivity of personnel and key systems.

The current level and strength of existing physical, administrative, and technical controls should be identified. An essential task is to determine if the principles of least privilege and separation of duties are being followed and enforced. For each identified role, the firm should ensure that the employee has only the level of access required to accomplish the job responsibilities and nothing more. It should examine whether critical functions are dispersed between two or more employees. Similarly, the firm should determine whether there are policies and procedures in place to enforce these principles.

What Employers Should Do Now to Combat Insider Threats

- Conduct a vulnerability assessment identifying reasonably anticipated insider threats. A vulnerability is any weakness in systems, security procedures, controls, policies or procedures or implementation that could be exploited by an employee or other insider.[9] The capability to cause exfiltration or unavailability of key information for each job position should be identified and evaluated.
- Next, conduct a well-documented risk assessment to assess the likely impacts (i.e., probable losses) that may result from an exploitation or attack involving the vulnerability, depending on the level of existing insider controls or those that are planned.
- Consider whether to add to or strengthen your insider threat controls consistent with the risk, firm's business needs, risk tolerance, and a cost-benefit analysis. Usually, for high-impact "critical" systems containing trade secrets, the full range of available, most protective physical, administrative, and

technical insider threat controls, consistent with applicable law, should at least be considered.

- Plan and implement a "defense in depth," selecting the proper combination of technical controls and workforce management practices and policies pursuant to a well-thought-out strategy of risk reduction. Consider, for example, a combination of enhanced background and credit checks, enhanced offer letters and onboarding procedures, electronic system monitoring, rigorous mobile device and remote access management, protective provisions in vendor contracts (e.g., requiring background checks), encryption, multi-factor authentication, human resources data/event logging (e.g., poor performance reviews/other indicia of employee disgruntlement), employee training (e.g., training in cyber security policies or recognizing potential attacks like phishing attacks), logical and physical separation of workforce users, periodic penetration testing, decrypting encrypted communications for monitoring to prevent exfiltration, and/or technical controls disabling external media (e.g., blocking access by employees to file-sharing cloud-based websites (like Dropbox), or disabling usb/external hard drive/printer functionality).
- Implement comprehensive acceptable use, access control, workforce monitoring and formalized employment termination/resignation policies and procedures because they are a "must have" for an effective "defense in depth" against insider threats. The policies and procedures should include measures to address well-recognized cyber security risks posed by workers: excessive consumer debt, dishonesty, poor judgment, gambling, criminal behavior, addiction or outside activities that pose a security risk.
- Monitor, log and maintain evidence of deviations from normal baselines across system usage and work habits.
- Comply with applicable law, such as the Fair Credit Reporting Act and the New York City Stop Credit Discrimination in Employment Act, which regulates consumer credit and background checks.[10]
- Put in place a written formalized incident response plan in case an insider threat materializes. This should include the processes and procedures to investigate the incident and mitigate damage. The plan should be tested through table-top exercises and should be a key component of the firm's efforts.
- Ensure that vulnerability and risk assessments of insider threats are conducted periodically and as financial services and other technologies evolve.

Endnotes

1. *See* Press Release, U.S Attorney's Office for the Southern District of New York, *Software Engineer Arrested for Attempted Theft of Proprietary Trading Code from His Employer* (Apr. 13, 2017) (https://www.justice.gov/usao-sdny/pr/software-engineer-arrested-attempted-theft-proprietary-trading-code-his-employer); Press Release, U.S Attorney's Office for the Southern District of New York, *Computer Engineer Arrested for Attempted Theft of Proprietary Trading Code from His Employer* (Apr. 7, 2017) (https://www.justice.gov/usao-sdny/pr/computer-engineer-arrested-theft-proprietary-trading-code-his-employer).
2. *See* Press Release, Patrick J. Fitzgerald, U.S. Attorney, *Former CME Group Software Engineer Indicted for Theft of Globex Computer Trade Secrets While Allegedly Planning Business to Improve Electronic Trading Exchange in China* (Sept. 28, 2011) (https://www.justice.gov/archive/usao/iln/chicago/2011/pr0928_01.pdf).
3. *United States v. Sazonov*, No. 1:17-cr-00657 (SDA), 2018 U.S. Dist. LEXIS 25943 (S.D.N.Y. Feb. 16, 2018).
4. *See United States v. Seoung Jeon*, No. 1:14-MJ-00054 (D. Del. 2015).
5. *See* 23 NYCRR 500.
6. *See* 16 C.F.R.§ 314.
7. *See* Press Release, National Association of Insurance Commissioners, *NAIC Passes Insurance Data Security Model* (Oct. 24, 2017) (http://www.naic.org/Releases/2017_docs/naic_passes_data_security_model_law.htm); Brian G. Cesaratto, *Model Cyber Security Law Pending Final Action by National Association of Insurance Commissioners*, Epstein, Becker & Green, P.C. (Oct. 19, 2017), https://www.technologyemploymentlaw.com/cyber-security-and-insider-threat-management/model-cyber-security-law-pending-final-action-by-national-association-of-insurance-commissioners/.
8. *See* ISO/IEC 27001: 2013; NIST SP 800-53r4.
9. National Institute of Standards and Technology, *Glossary: Vulnerability*, U.S. Dep't of Commerce (2018), https://csrc.nist.gov/Glossary/?term=2436#AlphaIndexDiv.
10. 15 U.S.C.§ 1681; N.Y.C. Admin. Code § 8-107.

Epstein Becker Green is an official Carnegie Melon University Software Engineering Institute Partner (SEI) and licensed to provide official SEI services in insider threat vulnerability assessments to organizations worldwide.

Brian G. Cesaratto is a member of the firm in the Litigation and Employment, Labor & Workforce Management practices, in the New York office of Epstein Becker Green. His practice focuses on cybersecurity and data privacy, computer and electronic data misappropriation, breach and forensics, technology and software licensing, internal investigations and litigation. Mr. Cesaratto is a Certified Information Systems Security Professional (CISSP).

Robert J. Hudock is a member of the firm in the Health Care and Life Sciences practice, in the Washington, DC, office of Epstein Becker Green. Mr. Hudock's practice covers data breach and response, national security law, cybersecurity, and global privacy and data security. Mr. Hudock is a Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH).