Published on *The National Law Review* https://natlawreview.com

Insider Threats to Critical Financial Services Technologies and Trade Secrets Are Best Addressed Through a Formalized Vulnerability and Risk Assessment Process

Article By:

Brian G. Cesaratto

The pace of innovative financial services technology is accelerating. Firms are investing heavily to develop the next cutting-edge financial services 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 individuals (e.g., a vendor’s workers) who have or may seek to gain access for a financial motive or other illegitimate purposes. Indeed, over this 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.

Financial services firms are, therefore, well served by utilizing a formalized vulnerability and risk assessment process to identify the insider threats to the confidentiality, integrity, and availability of their most critical technologies and systems and to address the risks. New York State registered or licensed financial services firms are required to conduct vulnerability assessmentsbiannually and risk assessments on a periodic basis. FTC-regulated financial institutions are also required to conduct risk assessments relevant to safeguarding non-public customer information.

Firms should identify their critical information systems and the supporting hardware and interconnected communication systems. The job roles associated with those systems—i.e., any insider who by virtue of his or her job position will be granted access—should be identified. In particular, managerial and other roles that involve privileged access to the systems should be pinpointed (e.g., database or network administrators). A map, chart, or other representation of the systems, data, and insiders should be made so that the organization can thoroughly understand the interconnectivity of personnel and key systems.

The insider threats to these systems for all roles should be identified and evaluated—e.g., is there a greater threat from temporary workers or third-party contractors not presently subjected to background checks as compared with full-time employees who undergo pre-employment credit and criminal background checks? The current level and strength of existing physical, administrative, and technical controls should be identified. An essential task is to determine if the principle of least privilege is being followed and enforced—e.g., for each identified role, does the insider have only the

level of access required to accomplish the job responsibilities and nothing more?

What Employers Should Do Now

- Conduct a vulnerability assessment identifying reasonably anticipated insider threats.
- Next, conduct a well-documented risk assessment to assess the likely impacts (i.e., probable losses) that may result from an attack depending on the level of existing controls or those that are planned.
- Consider whether to add to or strengthen your insider threat controls consistent with your business needs, risk tolerance, and a cost-benefit analysis. Usually, for high-impact “critical” systems, 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, electronic system monitoring, rigorous mobile device and remote access management, protective provisions in vendor contracts, encryption, multi-factor authentication, biometric identification, human resources data/event logging, employee training, penetration testing, and/or technical controls (e.g., blocking access by employees to file-sharing cloud-based websites (like Dropbox)).
- Put in place a written formalized incident response plan in case an insider threat materializes. The plan should be tested through table-top exercises and should be a key component of your efforts.
- Ensure that vulnerability and risk assessments of insider threats are conducted periodically and as financial services technologies evolve.

National Law Review, Volume VII, Number 333