Employer Data Breach Liability: The Employee as a Threat Vector

By Barry S. Herrin, JD, FAHIMA, FHIMSS, FACHE

“We have met the enemy, and he is us,” said famous cartoonist Walt Kelly. The phrase can easily be applied to healthcare privacy and security threats.

According to a 2014 IBM study, 31.5 percent of all cybersecurity incidents in 2014 were perpetrated by malicious insiders, and 23.5 percent resulted from the activities of non-malicious insider threats.[1] In 2017, statistics reported by the MIT Sloan Interdisciplinary Consortium showed an increase in the likelihood of insider threats. And a 2018 Ponemon Institute report confirms that this upward trend is not abating.[2]

Six Big Decisions in Human Resource Policies

With education having failed in many instances, and criminals becoming ever more sophisticated, perhaps employers should consider their employees threat vectors and not innocent victims in cybercrime. Some experts have concluded that a new model for protecting organizations is required. This article discusses six big decisions healthcare organizations should consider making in order to better protect themselves from insider threats.

Big Decision #1: Changing Training Focus from ‘Threat Prevention’ to ‘Patient Safety’

Changing the approach of cyber hygiene training in the healthcare environment from one of information technology to one of patient safety might yield significant improvement. Human resources decisions that align internal cybersecurity with patient safety initiatives could be more effective. Components of this approach, as frequently touted by security experts, might include:

- Empowering employees to report suspect behavior of others
- Providing a main emergency line to obtain responses for the “inadvertent click”
- Calling a “code” when suspicious cyber activity occurs
- Rewarding employees who respond favorably to training

Big Decision #2: Empower Employee Surveillance

In 2017, the US Department of Homeland Security and the Federal Bureau of Investigation published a reference aid on “Insider Threat Behaviors and Mitigation Responses.” Although this guidance was designed for the public sector, it is instructive to the private sector as well. The Insider Threat Reference Aid lists a series of suspicious activities that could be evidence of an insider threat and should be reported to management:

- Document collection, copying, or movement from one storage location on a system to another or onto portable media
- Any use of unauthorized devices, drives, or data storage media
- Unusually excessive or continuous printing of documents
- Carrying a computer, tablet, or briefcase when not previously required
- Maintaining or changing work hours in an abnormal way
- Excessive failed login attempts[3]

Separate and apart from other suspicious activities, potential insider threats display certain types of suspicious behaviors. These behaviors have been categorized in coordination with behavioral scientists at the Carnegie Mellon University’s Software Engineering Institute, and include:[4]

- Employees who are consistently disgruntled, angry, or perceive that workplace injustices routinely occur against them may be more likely to agree to engage in harmful behavior
- Employees who constantly manifest a feeling of being undervalued, underpaid, passed over for promotions, or who are not included in activities with others of their job level or seniority will begin to demonstrate a lack of regard for the organization
- Any persistent pattern of negative performance
- Employees who demonstrate a tendency to routinely violate workplace rules because they perceive themselves as better than their peers
- Employees who suddenly begin to display stress, anxiety, or anger in the workplace due to workplace or life changes
- Employees who exhibit changes in spending behavior or display signs of unexplained financial gain
- Employees with substance use, abuse, or dependency problems use stolen resources to support their habit, and knowledge of addiction can be exploited by outsiders to leverage the insider[5]

Big Decision #3: Treat Information Technology Access as a Privilege, Not a Right

Because we know what some of the common behaviors and activities are for a significant number of insider threat actors, human resource policies and practices should change to screen out those risks, both at initial hire and during the person's tenure at the enterprise. Some examples of these types of screening activities include the following:

- Thorough background checks on employees
- Employees with access to enterprise financial assets or customer credit card information should have credit checks at a minimum
- Apply the same screening criteria to full- and part-time employees, as well as to independent contractors
- Define access to information technology by role and include this role-based access in job descriptions
- Monitor access to information technology resources and set reasonable employee expectations to privacy
- When employees are promoted within the enterprise or gain new or different levels of access to information technology, resources, or datasets, mandatory rescreening should be conducted, according to National Institute of Standards and Technology identification and authentication control guidelines

Big Decision #4: Cutting the Cord to Social 'Notworking' Sites and Personal Email Accounts

The growth of social engineering-based targeted cyberattack should make every enterprise extremely wary of employee access to social media.[6] Information gained from social media sites can lead to targeted phishing attacks or even to criminal outsiders (or mischievous insiders) guessing an employee's passwords. Additionally, and as with any case of "cyber stalking," attackers can learn about an employee's workplace, his or her level of satisfaction with work, names of supervisors, and other information—making an intrusion attempt or an attempt to convert the employee to a willing participant in a criminal endeavor more successful. Finally, with access to personal social media sites and individual email accounts through the enterprise's internet channels, the enterprise's systems can more effectively be exposed to malware and to the easy ability of employees and others to exfiltrate enterprise data without much notice.

Some tips include:

- Employees need to be taught how cybercriminals use social media sites to engage in socially engineered exploits
- Enterprises should not permit employees to use commonly available personal information to reset internal passwords, such as ZIP code, mother's maiden name, place of birth, etc.
- Targeted phishing exercises can be used to illustrate how criminal actors gain access to systems and email accounts, thereby heightening employee awareness of the risk of "cross-pollination" between work and personal online presences.
- Robust employer policies should clearly describe how much online privacy an employee has when using employer IT resources
- Finally, employers should set parameters for what employer data (including employee-specific data) can be made public on social media sites

Big Decision #5: Incorporate IT Issues into the Termination Process

Once a decision has been made to fire an employee, human resources, physical security, and information technology departments need to collaborate on the termination process. When an employee leaves the enterprise, their position as a potential cybersecurity threat will persist.

Employers should take the following steps:

- Physical and cyber access to critical systems and spaces should be terminated at the time the decision to terminate is affirmed
- Keycards, passwords, and other tokens allowing access to employer resources should be disabled prior to the exit interview
- Any trusted devices issued to the employee should be removed from the list of such devices at the same time as the employee’s access to IT systems is removed
- When any employer-furnished devices are collected from the employee at the exit conference, forensic examination of those devices should be undertaken
- All keys, cards, workplace identification cards and badges, uniform items, and other means used to gain physical access to the employer’s spaces should be confiscated and accounted for
- The workforce should be informed of the employee’s termination, and reception and security employees should be given a photo of the employee accompanied by instructions should the employee appear at any employer workplace location

Big Decision #6: Deciding When to Shift from Education to Punishment

Employee negligence that causes a business either financial or reputational harm is almost always dealt with in disciplinary terms in every environment except the information technology environment, and only in healthcare is there an external audit and oversight structure that virtually mandates employee discipline for wrongful use or disclosure of a patient’s “protected health information.”[7] However, only in the most catastrophic circumstances are employees subject to significant discipline for violation of the enterprise’s email hygiene, password, and other polices designed to mitigate the risk of insider threat. Thus, it becomes a decision not whether to discipline or terminate an employee, but when. With over a decade of internal training on privacy, cybersecurity, typical cybercrime exploits, and the increasing prevalence of cyberattack in all industries, businesses must decide when enough truly is enough.

Notes

1. Kauh, Janghyuk et al. “Indicator-based Behavior Ontology for Detecting Insider Threats in Network Systems.” KSII Transactions on Internet and Information Systems. October 1, 2017. www.thefreelibrary.com/Indicator-based+Behavior+Ontology+for+Detecting+Insider+Threats+in...-a0521172143.
2. Ponemon Institute. “2018 Cost of Insider Threats: Global Organizations.” April 2018. www.observeit.com/ponemon-report-cost-of-insider-threats/.
3. Georgia Institute of Technology Applied Research Corporation. “Protecting Your Organization from Insider Threats.” March 30, 2017.
4. Collins, Matthew L. et al. “Common Sense Guide to Mitigating Insider Threats.” Carnegie Mellon University Software Engineering Institute. December 2016. https://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=484738.
5. Cassidy, Tracy. “Substance Use and Abuse: Potential Insider Threat Implications for Organizations.” Insider Threat Blog, Carnegie Mellon University Software Engineering Institute. April 12, 2018. https://insights.sei.cmu.edu/insider-threat/2018/04/substance-use-and-abuse-potential-insider-threat-implications-for-organizations.html.
6. Collins, Matthew L. et al. “Common Sense Guide to Mitigating Insider Threats.”
7. US Department of Health and Human Services. “HIPAA Administrative Requirements: 45 CFR Section 164.5309(e)(1).”

Barry S. Herrin (barry.herrin@herrinhealthlaw.com) is the founder of Herrin Health Law, P.C., a boutique law practice dedicated to the legal needs of the healthcare industry. This paper is an expansion of remarks given by Herrin at the DRI Data Privacy and Cybersecurity Law Institute in Chicago, IL in September 2018.

Article citation:
Herrin, Barry S. “Employer Data Breach Liability: The Employee as a Threat Vector.” *Journal of*

AHIMA 89, no. 10 (November-December 2018): 34–35, 58.

Driving the Power of Knowledge