August 2016

Do You Know Who Your Employees Are?

Insider threat is becoming one of the largest threats to organizations and some cyberattacks may be insider-driven. Although all insider threats are not malicious or intentional, the effect of these threats can be damaging to a Covered Entity and Business Associate and have a negative impact on the confidentiality, integrity, and availability of its ePHI. According to a survey recently conducted by Accenture and HfS Research, 69% of organization representatives surveyed had experienced an insider attempt or success at data theft or corruption. Further, it was reported by a Covered Entity that one of their employees had unauthorized access to 5,400 patient's ePHI for almost 4 years.

US CERT defines a malicious insider threat as a current or former employee, contractor, or business partner who meets the following criteria:

- *has or had authorized access to an organization's network, system, or data;*
- *has intentionally exceeded or intentionally used that access in a manner that negatively, affected the confidentiality, integrity, or availability of the organization's information; or information systems.*

According to a survey conducted by U.S. Secret Service, CERT Insider Threat Center, CSO Magazine, and Deloitte, the most common e-crimes committed by insiders are:

- *unauthorized access to or use of organization information;*
- *exposure of private or sensitive data;*
- *installation of viruses, worms, or other malicious code;*
- *theft of intellectual property.*

***Covered Entities and Business Associates should consider*:**

- Developing policies and procedures to mitigate the possibility of theft of ePHI, sabotage of systems or devices containing ePHI, and fraud involving ePHI. These policies and procedures should enforce separation of duties and least privileges, while also applying rules that control and manage access, configuration changes, and authentication to information systems and applications that create, receive, maintain, or transmit ePHI.

- Conducting screening processes on potential employees to determine if they are trustworthy and appropriate for the role for which they are being considered. Effective

screening processes can be applied to allow for a range of implementations, from minimal to more stringent procedures based on the risk analysis performed by the entity and role of the potential employee. Examples of potential screening processes could include checks of the HHS OIG LEIE (List of Excluded Individuals and Entities) to check for health care fraud and related issues and criminal history checks to verify past criminal acts. When implementing a screening process, please be sure to review and comply with any applicable federal, state or local laws regarding the use of screening processes as part of the hiring process.

- Following US CERT steps to protect ePHI from insider threats:

1. Consider threats from insiders and business associates in enterprise-wide risk assessments.
2. Clearly document and consistently enforce policies and controls.
3. Incorporate insider threat awareness into periodic security training for all employees.
4. Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
5. Anticipate and manage negative issues in the work environment.
6. Know your assets.
7. Implement strict password and account management policies and practices.
8. Enforce separation of duties and least privilege.
9. Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
10. Institute stringent access controls and monitoring policies on privileged users.
11. Institutionalize system change controls.
12. Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.
13. Monitor and control remote access from all end points, including mobile devices.
14. Develop a comprehensive employee termination procedure.
15. Implement secure backup and recovery processes.
16. Develop a formalized insider threat program.
17. Establish a baseline of normal network device behavior.
18. Be especially vigilant regarding social media.
19. Close the doors to unauthorized data exfiltration.

Resources: US-CERT http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34017