COSMOS
Navigate the Compliance Universe

Compliance Today - December 2018
Insider threats: Healthcare privacy and security

by Michelle O'Neill, MSJ, CHP

Michelle O'Neill (moneill@shm.net) is National Director, Corporate Compliance and Privacy Officer at Summit Health Management in New Providence, NJ.

In the privacy and security world of healthcare, data breaches are the number one threat. The impact of a data breach is felt throughout the entire organization and, many times, directly affects the patients of the organization. A phrase most often used when it comes to data breaches is, "It's not if, but when." As much as organizations do not want to face that reality, this isn't so far from the truth.

Although data breaches can be felt across all organizations, healthcare is at the top of the list. Most likely, this is because the value of the medical record is significantly higher than the value of any other data. Why are medical records more valuable to cyberthieves? Because they are harder to change or freeze. The other factor revolves around the reality that healthcare generally spends less on ensuring the privacy and security of this valuable information, making it an easier target as well.

The scariest factor in all of this is, the healthcare industry is the only industry where the threat from the inside is greater than the threat from the outside.[1] Verizon's 2018 Data Breach Report revealed that 56% of attacks are from internal sources (insiders). The report further detailed that human error is a major contributor, in addition to abuse of system access, but there is also the malicious component. It is very important to understand the types of insider threats, the causes and dangers of insider threats, and how to fight back and protect against these threats.

What is an insider threat?

An "insider threat" is a threat to an organization's security or information that comes from within. This term is often used to refer to employees, subcontractors, or vendors who maliciously or inadvertently use, damage, or disclose data. It is very difficult for organizations to believe that insiders would pose a threat, because insiders are the individuals that organizations put faith in to be loyal and look out for the best interests of the organization. Unfortunately, in many cases, that trust is betrayed.

Types of insider threats

According to Verizon's 2018 Data Breach Report, accidents accounted for the majority of the security incidents. This information is consistent with years prior, where human error was the major contributor. Accidental threats happen generally because the insiders may not be educated enough on privacy/security policies, procedures, and best practices. Employees also make mistakes, especially when many are multitasking in very busy patient care environments and are, at times, also short-staffed. Some examples of accidental threats include an employee who may click on a phishing email or malicious link. Although the 2018 report showed that only 4% of individuals will click on any given phishing campaign, attackers only need one individual to make a mistake in order to accomplish their mission and potentially cause a data breach. Other accidental threats include faxing accidents, where information is sent to the incorrect party or where a number is preprogrammed incorrectly, and

large amounts of patient information are sent to the incorrect place. And an email accident, where just one character is mistyped in an address, can lead to a serious Health Insurance Portability and Accountability Act (HIPAA) breach.

Another type of insider threat is negligence. These are the insider threats where an organization's employees do not pay attention to the policies that are in place to protect patient data. There is no malicious intent, but they could open the organization up to dangerous security threats. This can be as simple as leaving a logged-on computer unlocked. The word on the dark web is that average hackers take less than eight seconds to obtain all the patient data needed from an unlocked computer. It's that easy. Another example of negligence can be an employee or insider sending an email containing patient information via an unsecure account, which also can potentially lead to a big HIPAA breach.

The last type of insider threat is the scariest, and that is the malicious type. This is where individuals/employees inside the organization act with ill intent, because they may be motivated by financial gain or they are disgruntled. The following are some examples of malicious insider threats:

- A disgruntled employee may extract sensitive data and sell it on the black market or release it publicly;
- An employee may access friends' or family members' charts for curiosity and/or to do harm;
- A physician may be leaving an organization to start up his/her own practice and may "steal" patient information lists;
- An employee may sell information about a "high-profile patient" to media outlets for financial gain;
- Employees may post patient information on social media.

Although malicious threats are not the major contributor of insider threats, these are the threats that organizations need to pay the closest attention to, because they tend to cause the biggest security breaches out there, and they are very expensive. These threats also cause reputational damage that is often hard for the organization to recover from.