Things Privacy Officers Can Do Today to Defend Against a Cyberattack

By Marti Arvin, JD

One might ask why a privacy officer even needs to worry about defending against a cyberattack—isn't that the role of the chief information security officer and the chief information officer? The answer is no. Cyberattacks are not always about technology. The privacy officer is not generally responsible for the strength of an organization's technology solutions, like the firewall, the selection and deployment of its anti-virus software, or the myriad of other technology features that can help protect an organization against a cyberattack. However, that does not mean the role is not key in helping defend against a cyberattack in other ways.

Synchronize Education and Training

The roles of privacy officer and chief information security officer should be working together, particularly in the area of education. One of the weakest links in the defense against a cyberattack is the individual workforce member. The privacy officer should be involved in the development and deployment of training and education for the workforce to help ensure they know the key ways cybercriminals can get into the organization (i.e., phishing e-mails, malware, failure to patch systems, etc.).

Cybercriminals may also use subtler, non-technical methods for gaining access to an organization, such as social engineering. If an employee lets someone into a secure area without asking for identification or requiring the individual to sign in at the security desk, this may allow unauthorized access to secure areas. These areas often have sensitive information, like patient information, but could also contain information about an organization's system structure that identifies vulnerabilities.

If the education of the workforce is primarily led by the chief information security officer, the privacy officer should still be involved and have input on content. This coordinated effort also helps ensure a consistent message. Conducting privacy training in a vacuum from the information security training can result in unintentional confusion in the messaging and duplication of effort. Coordinating the effort and getting the message out so that workforce members are exposed to the different and sophisticated ways a cybercriminal might present themselves can help deter their entry into the organization's environment.

Provide Support and Advocate for Needed Resources

Protecting against a cyberattack is seldom foolproof even in the best of circumstances. Understanding the risks an entity faces is a key factor to mitigating risk. If you don't know it's broken, how will you fix it? The privacy officer should have a working understanding of the results of the organization's privacy and security risk assessment. The individual should be a part of the team advising senior leadership on the priority of the risks identified and methods for remediating high risk items. By understanding the risks and the remediation plan, the privacy officer can be an additional resource to reinforce the need for strong cybersecurity protections.

The privacy officer may also be a key asset if he or she can serve as a translator. It is not uncommon for the IT staff to use technical jargon. This can cause the understanding of an issue, the way to fix an issue, and reasons the fix is necessary to get lost. Translating the more technical jargon IT folks use can make the critical difference in leadership understanding the risk. Key decisions must be made about short-term and long-term fixes for identified cybersecurity risks. If the senior leadership does not fully understand the nature of the risks because the technical jargon is over their heads, then these decisions may not be made in an informed manner.

As a resource to senior leadership, the chief information security officer and chief information officer can help increase the understanding that allows for a more informed decision. Being an advocate that understands enough about what IT is saying and being able to translate that to a more layperson-friendly message helps ensure that the governing body understands the importance of proposed changes that will likely mean significant resource commitments.

Incident Response Preparedness

Being prepared to respond to a potential or actual cyberattack does not sound like much of a way to defend against it. However, being well prepared can help limit the spread of an attack. The privacy officer should be part of the incident response team. The privacy officer role is one that should be helping make key decisions such as whether to take a device, server, or system offline once an intrusion has been detected. Understanding the criticality of systems and the consequences of taking something "offline" before the event happens may be the key to stopping a cyberattack from perpetuating. Gaining that knowledge of the systems and applications beforehand will permit a prompt decision in a situation where time is of the essence.

Being prepared for something like a ransomware attack by identifying the differing responses that the organization will consider allows for a more controlled response. The organization may determine that it will respond differently if the ransomware is impacting one machine versus a critical segment of the IT infrastructure or the entire network. The privacy officer should play a key role in helping the organization prepare for this.

Creating an offensive posture will help an organization defend against a cyberattack. The privacy officer is a key player in coordinating and planning the organization's efforts to engage in actions that help minimize the risk of a cyberattack occurring. The role is also key in planning what to do when an attack occurs. That said, the privacy officer can typically leave implementation of the technical solutions to the chief information security officer and the chief information officer. But he or she should be aware of what those solutions are and how it helps the organization minimize risk.

Marti Arvin (marti.arvin@cynergistek.com) is vice president, audit strategy, at CynergisTek, Inc.

Article citation:
Arvin, Marti. "Things Privacy Officers Can Do Today to Defend Against a Cyberattack" *Journal of AHIMA* 88, no.4 (April 2017): 22-23.