Evolving Role of the Privacy and Security Officer

Save to myBoK

By Rita K. Bowen, MA, RHIA, CHPS, SSGB

Fifteen years ago, many individuals accepted the role of the privacy officer with a perception that it would be a role involving the education and training of individuals on HIPAA rules and regulations, developing policy, and responding to reported incidents. The security officer was focused on system integrity and may or may not have been actively involved in systems access approval. Their role and focus was most likely centered on information controlled in the data center, and primarily focused on detection and protection of that domain.

Today these roles require a constant awareness of the ever-changing landscape that determines how health information is used and shared. As organizations prepare their information governance plans, privacy and security officers must be included to map out what data elements are transferred among systems and validate the appropriateness and security of the processes.

The focus of privacy and security is how to meet information access demands while still maintaining the sensitivity of the information being shared. Along with existing federal regulations for health information protection, 47 states have versions of their own rules and regulations for breach notification. States may also have their own definition of when an incident is a reportable breach.

High-Profile Breaches Alter Security Mindsets

A lesson learned from the breaches of 2014 is that an organization cannot be over-prepared. High profile breach incidents involving Anthem, Target, and Home Depot proved that traditional security solutions are not effective. Every reported incident should be evaluated and used as an opportunity to identify where privacy and security gaps might exist and how they should be resolved.

Privacy and security officers need to think like a thief and determine what data elements are vulnerable and how that information can be used for personal gain—then figure out a way to protect against those threats. Organizations must identify the continuing advanced techniques for intrusion that defy detection by traditional security solutions. Privacy and security officers must stay constantly aware of regulations and penalties that may result in reputational harm as the result of an incident.

Privacy and security compliance officers should report directly to the organization's CEO and board of directors as these positions must be vigilant about the organization's environment and create a strategic approach for that environment to be managed. This can be accomplished by conducting frequent environmental scans, which can help organizations be continually prepared to respond to security threats or breaches. Examples such as the breach reported by insurer Anthem in 2014 that impacted millions of people has shown the industry that timelines are important, as is recording each item reviewed, how a decision was made, and the resulting outcome. How an organization manages its response to incidents is also paramount.

Managing Incident Response

It is vital that privacy and security officers have a thorough and complete plan in place for when an incident is reported. It must be timely and consistent in the analysis and reporting of mitigation efforts. Whether there is a single response plan of action, ad-hoc committee response type action, or a fully active privacy and security incident response team, the response timeline is essential. The timeline is reduced if an organization has a privacy and security incident response team that has predefined roles and action requirements. Every event should result in a post-mortem review to determine if improvements in the review and response timeline can be realized.

A clear definition of all roles involved in that process is necessary to help ensure an organization's success following the unwelcome attention that comes from a breach. The breach incidents reported in the media last year led to some top executives losing their jobs because the incidents were handled poorly within their organizations.

Privacy and security officers should be focused on organizational objectives that are audited for effectiveness, and reported to executive leadership and the board of directors. The processes must be consistent, repeatable, and manageable. Incident response should include:

- Discovery of the incident
- Timely reporting of said incident
- Containment of the incident
- Investigation
- Documentation assessment
- Notifications

For each incident it is important to break down the human factor. According to a recent Ponemon Institute report, human errors and system problems caused two-thirds of data breaches in 2012.[1] An Ernst and Young analysis found similar results.[2] Thirty-eight percent of respondents said employee carelessness or lack of awareness was the primary threat that increased their exposure risk.

Both the nature and sheer volume of data have evolved and grown at a rapid pace over the last two decades, and that trend will likely continue. According to Cisco, global IP traffic has increased fivefold over the past five years, and will increase threefold over the next five years.[3]

So yes, the jobs have changed, but the continued focus must be on education of the individuals working within the organization and those handling the information that privacy and security officers have been entrusted to protect.

Notes

[1] Ponemon Institute. "Cost of a Data Breach: Global Analysis." June 1, 2014. www.ponemon.org/library/2014-cost-of-data-breach-global.

[2] Prince, Brian. "Cybersecurity Requires Proactive Approach: Ernst & Young." *Security Week*. November 3, 2014. www.securityweek.com/cybersecurity-requires-proactive-approach-ernst-young.

[3] Cisco. "Cisco Visual Networking Index: Forecast and Methodology, 2013-2018." June 10, 2014. www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html.

Rita Bowen (Rita.Bowen@HealthPort.com) is senior vice president of HIM, privacy officer, at HealthPort.