Managing Data Protection and Cybersecurity—Audit’s Role

Data protection and cybersecurity go hand-in-hand due to the nature of the risk involved. The underlying assumption is that all data, whether they are stationary or in motion, are threatened to be compromised.

A prime example of this can be seen in the medical device industry. Due to the explosion of medical device innovation, resulting in both economic and consumer/patient health advancement, the industry has seen a growing number of threats from a cybersecurity risk landscape. The US is the largest medical device market in the world with a market size of approximately US $110 billion, and it is expected to reach US $133 billion by 2016. The industry has seen a rise in innovation since the early 2000s, primarily due to the advent of technological advancement and the demand from consumers and health care practitioners to further the quality of the patient care provided. A few of the relevant, more commonly known medical devices are pacemakers, infusion pumps, operating room monitors, dialysis machines—all of which retain and potentially transmit vital patient and equipment data to medical professionals and other sources gathering data.

Security experts say cybercriminals are increasingly targeting the US $3 trillion US health care industry, in which many companies remain reliant on aging computer systems that do not use the latest security features. As a result, the percentage of health care organizations that have reported a criminal cyberattack rose to 40 percent in 2013 from 20 percent in 2009, according to an annual survey by the Ponemon Institute think tank on data protection policy. As revealed in the 2014 Cost of Data Breach Study: Global Analysis, sponsored by IBM, the average cost of a breach to a company was US $3.5 million dollars, 15 percent more than what it cost the previous year.

The role of IT security professionals, especially in the audit function, is to be the front line in identifying and helping to address the risk that enterprises face in the growing threat landscape operating at a global level. As a result, every audit function should consider spending time on identifying opportunities to perform a review around data protection and cybersecurity within its respective enterprise to help identify gaps and work with key departments in the enterprise to help reduce and/or eliminate the gaps as best as possible.

**RISK ASSESSMENT**

To begin, enterprises should consider performing a risk assessment of the threat landscape; making this happen starts with the tone at the top. The risk assessment normally should be owned by the enterprise-level functions, and it can be a joint effort between the audit function and the business functions in an effort to ensure that there is synergy between the two. Risk assessments are meant to help identify and address the gaps that may be exacerbated in the event of a cyberrisk due to a lack of key controls. One of the primary resources for creating an internal risk assessment analysis of an organization is the framework provided by the American Institute of Certified Public Accountants (AICPA). The AICPA has drafted a white paper that attempts to simplify the practitioner's understanding of the risk assessment standards and process by focusing on the end game and how that objective can be achieved in an effective, yet efficient, manner. An effective way to simplify the risk assessment is by dividing the areas of the assessment into the following categories (figure 1):

- **Understand the business.** It is vital to include the fundamentals of the organization from the top. This includes knowing who the customers are and what the key products are that drive the very engine of the enterprise. One of the best resources for US companies to utilize to further the organizational knowledge is to review Form 10-K, an annual report required by the US Securities and Exchange Commission.
Commission (SEC). This gives a comprehensive summary of a company’s financial performance. It can help further an understanding of the enterprise based on the knowledge already amassed and enable a view of the risk from a business and financial perspective.

- **Know the organization’s internal control environment.** Elements of a strong internal control environment include the right combination of IT and transactional-level controls that are backed by a process to manage the reporting of any breakdown of controls and actionable plans stemming from such a breakdown. The DNA of the internal controls of an organization is composed of the philosophy, adaptation, integrity and stance of the organization’s resources toward the control environment.

- **Collaborate among departments.** The audit function has one of the best positions in the company when it comes to bringing together various departments to collaborate on all aspects of key business, financial and regulatory risk—both internal and external. Collaboration among the chief privacy officer (CPO), chief information security officer (CISO), chief audit executive (CAE) and chief risk officer (CRO) is vital to have a robust risk assessment program in place.6

- **Summarize and communicate the risk assessment.** Risk communication is commonly defined as the “process of exchanging information among interested parties about the nature, magnitude, significance, or control of a risk.”7 It is important to include all the key stakeholders of the organization as part of the risk assessment summary of recipients, which should be ideally communicated for each key business and function, as well as at the enterprisewide level. This helps with the delivery and the overall execution of the proposed audits that are planned for the year and in paving the way for having a robust audit plan clearly defining the audit and the risk that correlates to why the audit is being conducted.

**DATA PROTECTION AND CYBERSECURITY AUDIT SCOPE**

To have a meaningful scope for an audit around data protection and cybersecurity, one must consider all relevant areas of the organization that require inclusion in the scope of the audit. The functional entities that ought to be considered in scope should include customer operations, finance, human resources (HR), IT systems and applications, legal, pharmacovigilance, purchasing, regulatory affairs, environmental/physical security, and all applicable vendors or third parties in any of these areas. Specifically, for each of the areas, the auditor should consider the following areas as part of the audit:

- **Key IT systems and applications located in the local data centers:**
  - Verification of the security management of the systems and applications, including the logging and monitoring of systems containing sensitive data

- **HR (full-time and temporary labor):**
  - Recruitment and vetting of candidates for key roles within the organization that have access to highly confidential data
  - Management of the on-boarding process and proper training and compliance monitoring as needed for specific roles, while paying attention to company and country laws around employee rights and privacy
  - Off-boarding process of employees and agreements of noncompete and confidentiality of organizational and product intellectual property

- **Internal collaboration tools management:**
  - Enterprise content and document management (ECDM) system usage and data handling:
Verification of the overall management of data within the organization that are shared among peers on collaboration tools and platforms
- File share management:
  - File management and permissions on massive file shares utilized by the organization’s departments, the protection of the file shares via proper system administrative authorities, and monitoring of key file shares
- Third-party interaction and data sharing:
  - Contract management end-to-end life cycle, including standard language of key vendors that would have access to highly confidential data, including patient health information and intellectual property
- Personal computer device physical protection and encryption:
  - Internal and external technological controls necessary to deter flight of data from employees and/or contractors
- Records storage and management:
  - Onsite and off-site physical security of confidential paper data, including electronic tapes if off-site storage is utilized for backup purposes
- Incident response and handling:
  - Electronic asset management of key devices, including laptops, desktops, servers and mobile devices:
    - End-to-end life cycle of asset loss and disposal process

CONCLUSION
Data protection and cybersecurity management is a key area that all organizations have to manage well. A CIO Network event held by The Wall Street Journal included a panel of CIOs who prioritized a set of recommendations to drive business and policy in the coming years. Cybersecurity was one of the key themes that came out of the event and corresponding special report.

A primary responsibility for a CIO or CISO when talking to the chief executive officer (CEO) or board of directors (BoD) is to articulate how cybersecurity translates into revenue. Putting monetary value on security events and tying security to real-life business cases can show senior executives the potential impact of a cybersecurity event in terms that make sense to them.8

The role of audit is to embrace the function it plays as a key member of the organization that has to independently assess the organization’s management of risk around data loss and prevention by performing robust risk assessments at the organization level and delivering meaningful data protection and cybersecurity-related audits. This will help further the chance of an organization’s maturity level to increase when it comes to fighting the ever-growing threat of cyberespionage and internal malicious data loss through organizational employee resources and temporary labor workforces.

ENDNOTES

1 SelectUSA, “The Medical Device Industry in the USA,” http://selectusa.commerce.gov/industry-snapshots/medical-device-industry-united-states
4 While the AICPA framework is generally used for financial statements, it has proven to be a valuable framework for the general management and creation of guidance that embodies a generic model for other risk assessments—those that are not necessarily related to financial statements.