CFO Consulting Partners LLC
Cyber Security White Paper
March 2015

Cyber Security: A fundamental component of Enterprise Risk Management (ERM)

Cyberattacks have hit virtually every industry and the two industries most impacted by incursions, breaches and theft of data are financial services and health care. Financial services and the medical world are inexorably connected to the internet, and they are therefore connected to hackers, cyber criminals and even nation states intent upon getting access to financial and medical records.

Banks are a particular focus of cyber criminals. In a recent speech OCC Head Thomas Curry said," The financial-services industry is one of the more attractive targets of cyberattacks, and unfortunately the threat is growing." Further, one growing area of concern is the potential for criminals to target smaller banks. In late 2014 New York State banking regulator Benjamin Lawsky asked the institutions he supervises to understand the increasing complexity and interconnectedness of the financial system, as well as the importance of strong controls and of carefully monitoring the ways in which they connect to third parties.

Banks routinely use advanced statistical models and behavior analytics programs that can spot possible fraud and, to some extent, have a cultural data governance advantage over other industries. Analysts at the Gartner research group estimate that the health care industry is generally about ten years behind the financial services sector in terms of protecting consumer information.

In the healthcare world, major cyber breaches go back to 2010 when the WellPoint medical records breach set two records: the number of members' records exposed in a security breach, and the size of the settlement amount paid to the Federal Government. The WellPoint breach is estimated to have cost $143 million dollars. These costs were for legal recovery actions, new security control investments, and extended credit and protection services for victims. During an investigation of WellPoint's information systems, The US Department of Health and Human Services (HHS) found that the Indianapolis-based insurer had not enacted the appropriate administrative, technical and physical safeguards for data which are required Health Insurance Portability and Accountability Act of 1996 (HIPPA).

More recently the dangers of health care cyberattacks were highlighted early in 2015 when Anthem, the nation's second-largest health insurer, said hackers broke into a database storing information on eighty million people. The hack led to a particularly valuable trove of data because it exposed Social Security numbers.

Basic components of cyber controls framework, and ERM (Risk Management):

- Governance: Cyber Security Companies in all industries need to establish a cybersecurity governance framework which is a central component of the ERM infrastructure. Regular reporting to the Board of Directors will help assure active participation among the Board, Senior Management and IT Management. The visibility of the cybersecurity infrastructure and processes are an important driver of adequate resourcing, which is essential for companies to stay ahead of the many bad actors in the cyberattack world.

- Cyber Risk Assessment: Through risk assessments, companies understand the specific risks to their organizational infrastructure and operations. Risk assessment processes identify and document vulnerabilities, highlight internal and external threats, and ultimately prioritize the risk and related responses. The related controls should be organized and implemented as preventive, detective and corrective.

- Technical Controls: The selection of specific controls by any company is dependent the company's individual risk profile. Many companies use a "defense-in-depth" strategy in which they layer multiple independent security controls strategically throughout their technology systems. One way of looking at this approach is to view the components of a company's technical infrastructure as residing in partially redundant layers.

- Vendor management: At every touch point vendors can introduce cyber threats (e.g. – viruses) into a company's systems and data bases. While third party penetration testing is almost impossible with vendors, the company's threat assessment must thoroughly evaluate each third party touch point for cyber risks.

- Incident Response Planning: An incident response plan is a framework to manage a cybersecurity event and limit the damage. A company's incident response plan should establish a dedicated Cyber Security Incident Response Team, address all the possible attack vectors and take the legitimate concerns of third parties into account.

- Staff Training: Without adequate staff training and related awareness, the rest of a company's cybersecurity program can be easily compromised. Companies must define cybersecurity training needs and requirements. Staff need to understand the possible vectors and techniques that the bad actors use to penetrate systems and data bases.

- Cyber Insurance: While almost unknown five years ago, many companies have chosen to obtain cyber risk insurance. Coverage is offered my most major insurance underwriters; premiums vary widely. Underwriting relies heavily on the quality of a company's cyber control infrastructure. In other words, insurance premiums depend greatly on the quality and strength of the company's cyber control infrastructure.

Note: Cyber Control Framework items above extracted from FINRA 2014 "Report on Cybersecurity Practices".