Cybersecurity and the Evolving Demands for Chief Information Security Officers (CISO)

March 2018

What is a CISO?

Cybersecurity is a hot topic for today's senior leadership, directors, banks, lenders, financial services entities and consumers alike. Fueled by very public news headlines, significant cyberattacks impacting large companies such as Target, Sony and Equifax have raised awareness regarding the nature and magnitude of the current cyber threat. In fact, in 2017, the CFO Global Council, a group of diverse professionals established by CNBC, named hacking as the number one external risk factor facing companies today, replacing customer demand. Post-breach, companies face significant fines, penalties and other remediation costs, not to mention public scrutiny.

Behind the news headlines is the reality that companies must develop or reevaluate their cybersecurity strategy to address these threats. Creating a holistic strategy that attempts to identify vulnerabilities, risks and threats to the organization, while also identifying solutions aimed at reducing these risks and the associated legal and financial impacts going forward, is critical in today's business environment.

Reduced financial impact is the main driver for the development of a comprehensive cybersecurity strategy. Having a strategy that enables a business to operate while reducing risk requires strategic leadership: enter the Chief Information Security Officer (CISO). The role of the CISO can be traced back to 1995 when Stephen R. Katz was appointed to lead a global cybersecurity program at Citibank. Katz was appointed to the role after serving as the VP of IT Services for JP Morgan Chase, a role which was created in the wake of a $10 million-dollar loss. This significant monetary loss resulted from the manipulation of the cash management computer system, enabling the hacker to wire money into a number of his own personal accounts.

The role of a Chief Information Security Officer is to act as the head of cybersecurity, developing and implementing strategies that enable and protect the organization from cybersecurity risks such as information disclosure, ransomware, phishing, wire fraud and other hacking trends. A recent study of 184 mid-market and enterprise-sized organizations by the Ponemon Institute found that nearly 60% of companies today feel that cybersecurity is a key business priority, with 45% of them significantly concerned about a cybersecurity breach (Ponemon Institute, The Evolving Role of a CISO, August 2017).

A Day in the Life of a CISO

The key responsibility of a CISO is to ensure the successful execution of the cybersecurity operations and strategic plan. Essentially the CISO has the responsibility to ensure the confidentiality, integrity and availability of information assets that enable an organization to function.

In August 2017, a survey found that **58% of organizations** felt that their cybersecurity program and function had been developed independently **with little or no focus on the objectives or business needs** of their organizations. These independently-created plans were also found to create silos and political discourse within nearly 40% of those organizations. By developing a comprehensive plan in conjunction with senior leadership and key stakeholders of the company, a CISO is able to prioritize issues such as business continuity, incident response, and the implementation of technical and operational security controls that align with business objectives and compliance and regulatory requirements.

Other functional roles of a CISO include:

- Acting as a liaison between key stakeholders within the organization, such as management, IT, external vendors and the cybersecurity team
- When an incident occurs, being the central point of contact to ensure the investigation is reported and managed correctly
- Leading education and awareness across the organization

In order to successfully execute these tasks, a CISO must not only be continuously aware of on-going trends, vulnerabilities and mitigation strategies, but must also act as a strong communicator with a strong customer focus, able to tailor the message based on the audience. By forming strategic partnerships across the organization, the CISO is able to be a key advisor, helping make informed decisions about business operations and how to manage any associated cyber risk. And by being flexible and adaptable, a CISO is also able to develop alternative solutions that both meet the needs of the organization as well as reduce and manage risk to an acceptable level established by the senior leadership team.

Regulatory Pressure

In response to the growing trend of cybersecurity breaches, a number of regulatory and legal requirements have evolved, placing additional pressure on financial services companies, their cybersecurity strategy and ultimately their bottom lines.

Effective March 1, 2017, financial services and insurance companies licensed in the State of New York must comply with the Department of Financial Services Cybersecurity law, 23 NYCRR 500. While there are some limited exceptions to this regulation based on size and gross revenue, section 500.04 requires each covered entity to "designate a qualified individual responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Part, 'Chief Information Security Officer' or 'CISO'). The CISO may be employed by the Covered Entity, one of its Affiliates or a Third-Party Service Provider."

A number of other states are also looking to enact legislation focused on cybersecurity, including Massachusetts. The proposed law, Massachusetts - HB 2813, "requires companies that acquire, manage or retain financial data of individuals who reside in the commonwealth of Massachusetts to have a defined cybersecurity program that focuses on the People, Processes and Technology that is managed by a designated individual(s) capable of managing such a program." The law also states that the designated individual must be qualified, retained or hired by the regulated organization.

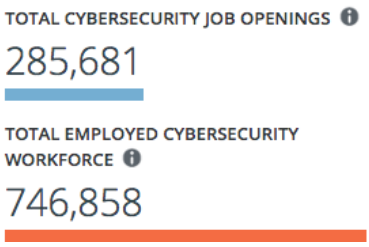
Federal agencies are also looking to implement cybersecurity regulations, including the U.S. Securities and Exchange Commission (SEC), and the agencies that focus on the financial services sector, the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC). The SEC's Office of Compliance Inspections and Examinations (OCIE) cybersecurity review guidelines specifically look for regulated organizations to not only have a formally documented and managed cybersecurity program, but to also name a CISO or equivalent position. And while not yet finalized, the regulations in development by the CFPB and FTC are also anticipated to require a designated CISO-type position, either hired by the regulated entity or retained from a qualified third party.

Globally, the European Union is focused on protecting the personal information of citizens of the EU through the General Data Protection Regulation (GDPR). The GDPR requires any company collecting digital information, such as website visitor data, cookies, customer name, address, and other personal identifiable information, to protect the confidentiality, integrity and availability of that data. The scope of the GDPR includes EU citizens living in or doing business in the United States. Organizations must have a privacy statement on what personal information they are collecting, as well as name a Data Protection Officer (DPO) to oversee the execution of the program.

All of these legal and regulatory guidelines share a common focus: a qualified individual must be defined to **manage and maintain a focus on cybersecurity**.

Finding the Purple Unicorn

In 2016, the average cost of a cybersecurity attack was estimated by researchers at the Ponemon Institute to be $154 per impacted record, with the average cost of $4 million per incident. The combination of costs, regulatory pressure, and the increase in demand for CISOs across all industries, particularly financial services and healthcare, has caused salaries to increase at a surprising rate. This has led to companies struggling to not only hire qualified CISOs, but also to retain that talent.



Today, **Cyberseek**, on online partnership between the National Institute of Technology and Standards (NIST), the United States Department of Commerce, and CompTIA, has found that nearly a quarter million cybersecurity roles are currently unfilled in the United States. Many experts trace the increase in demand back to 2013, with the very public Target and Home Depot cyber incidents. **A study by SilverBull, a full-service IT and cybersecurity recruiting firm, found that the average salary for a qualified CISO starts around $204,000, tipping as high as $380,000 in high demand markets such as New York, Washington DC, and San Francisco**. Additional research completed by Salary.com found similar data, adding that the average bonus for a CISO was **20-25%**, with many opportunities including signing bonuses and other additional perks.

The continued increase in salary has led to a vacancy rate for the position at an estimated 60% nationwide, as individuals often leave to take new positions with significant pay increases after a short 16-24-month tenure. The result of this musical chairs routine is a lack of stability and success in establishing and maintaining a comprehensive cybersecurity program. As the CISO moves on, a gap is presented in leadership, potentially derailing projects and the overall strategic progress. Even more dangerous to the organization is that with a new CISO often comes an entirely new cybersecurity program, stopping all progress and starting over, losing valuable time and resources.

Another Path Forward

Nearly a quarter of all cybersecurity incidents impact mid-market financial services companies. Not only can a cybersecurity incident be costly, but reducing your risk exposure and ensuring compliance can also be expensive. Utilizing an industry-specialized consultant can be an attractive solution to develop a best practices security program without the expense of a full-time employee. Largely handled remotely, virtualized CISO services provide both the development of and oversight over an end-to-end cybersecurity program for a fraction of the cost and without the risks associated with turnover in this role. For those companies who are required to define a CISO, virtualized CISO services ensure compliance and help leadership make informed decisions about managing cyber risk and the associated legal and financial threats to the organization.

Richey May's cybersecurity advisory and compliance services help financial services organizations address their People, Process and Technology to achieve compliance and reduce risk. Our virtualized CISO services are designed to create a baseline evaluation of your cybersecurity posture, and develop and ensure your strategic plan reaches and maintains maturity, while working with existing staff and vendors. Please reach out to **JT Gaietto**, Executive Director, Cybersecurity Services for additional information.