NAVINT

Cybersecurity and the Threat to Your Company

A Navint Partners White Paper

September 2014

Executive Summary

Cybersecurity is at the forefront of the global agenda. With multiple regulatory bodies focusing on the effectiveness and sophistication of a firms' cybersecurity infrastructure, firms need to be ready to prove that they can keep customer information safe even if they never encounter a breach.

In 2014, the White House stated that "cyber threat is one of the most serious economic and national security challenges we face as a nation," and that "America's economic prosperity in the 21st century will depend on cybersecurity." As you will read below, the Financial Industry Regulatory Agency (FINRA) and the Securities Exchange Commission (SEC) are developing controls over cybersecurity and developing assessment and examination programs to ensure that cyber risk is being mitigated adequately to protect sensitive financial and personal data. Frank Murphy, Managing Director of TBG Security Inc., states "the new rules and guidelines are an extension of what should already be best practice for a company. Companies should approach the implementation and strengthening of their cybersecurity plan as an integrated program across the entire company."

We will present the various approaches that these regulators are taking, give examples of the types of breaches they're attempting to stop, and then explain how we can assist your company in designing, building, and testing a solid approach to secure your most sensitive information.

Launch of the Cybersecurity Framework

The Government Sets the Tone for Controlling the Cybersecurity Threat

In February 2014, the U.S. introduced the Cybersecurity Framework. This guide is the product of the collaboration between private industry and the public sector. Industry leaders, as well as political leaders, indicated that the Framework is just the first step in creating a cybersecurity program for the nation's 16 critical infrastructure sectors. The implementation of this Framework is strongly encouraged but is voluntary at this point for unregulated industries.

Each component of the Framework (the Framework Core, Profiles, and Tiers) connects business drivers and associated cybersecurity activities.

An illustration of how an organization should manage its cyber risk is presented as Appendix A.

FINRA is Focusing on the Cyber Threat

FINRA announced that during the 2014 examination of its members, it will be conducting an assessment of its member firms' approaches to managing cybersecurity threats. FINRA is conducting this assessment in light of the critical role information technology (IT) plays in the securities industry, the increasing threat to firms' IT systems from a variety of sources, and the potential harm to investors, firms, and the financial system as a whole that these threats pose.

FINRA has outlined four broad goals in performing this assessment for each of its members:

- Obtain a better understanding of the types of cyber threats
- Determine the members' risk appetites, exposure, and major areas of vulnerabilities in their IT systems
- Determine whether the members are managing these threats
- Share observations and finding with the members

Note – The assessment addresses a number of areas related to cybersecurity, including a firm's:

- approach to IT risk assessment;
- business continuity plans in case of a cyber

attack;
- organizational structures and reporting lines;
- processes for sharing and obtaining information about cybersecurity threats;
- understanding of concerns and threats faced by the industry;
- assessment of the impact of cyber attacks on the firm over the past 12 months;
- approaches to handling distributed denial of service attacks;
- training programs;
- insurance coverage for cybersecurity-related events; and
- contractual arrangements with third-party service providers.

The SEC has Finalized its Cybersecurity Rules

In a March 2014 speech, SEC Commissioner Louis A. Aguilar stated, "In recent months, cybersecurity has become a top concern to American companies, regulators, and law enforcement agencies. This is in part because of the mounting evidence that the constant threat of cyber attack is real, lasting, and cannot be ignored."

SEC and Commodity Futures Trading Commission (CFTC) Rules

At the end of 2013, the SEC and the CFTC jointly issued final rules and guidelines to require certain regulated entities to establish programs to address risks of identity theft. These rules and guidelines implement provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act. The final rules provide that each financial institution or creditor that offers or maintains one or more customer account types must develop and implement a written program designed to "detect, prevent, and mitigate identity theft." The rules require financial institutions or creditors to follow these four major themes:

1. Develop a program that includes reasonable policies and procedures to identify relevant red flags
2. Develop reasonable policies and procedures to detect the red flags that the program incorporates
3. Develop reasonable policies and procedures to respond appropriately to any red flags that are detected
4. Develop reasonable policies and procedures to periodically update the program to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft

Administration

- The final rules provide that financial institutions and creditors must involve, and must gain approval of the initial written program from, either the board of directors, an appropriate committee thereof, or designated senior management
- Final rules provide that financial institutions and creditors must train staff, as necessary, to effectively implement their program
- The rules provide that financial institutions and creditors must exercise appropriate and effective oversight of service provider arrangements

The SEC will examine cybersecurity preparedness

In April 2014, the SEC announced that they will "assess cybersecurity preparedness in the securities industry and [will] obtain information about the industry's recent experiences with certain types of cyber threats." As part of this initiative, the SEC will conduct examinations of more than 50 registered broker-dealers and registered investment advisers, focused on the following: the entities' cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats.

For example, the documentation the SEC will be requesting may include:

- IT security policies and procedures
- Network maps
- Organizational charts (including the identification of the information officer)
- The information policy
- Remote access policies
- A risk analysis of customer confidentiality
- A map of connections and data flows (especially points of external connections)
- A business continuity plan that specifically addresses how the firm will handle the a possible
- Cybersecurity incidents, how the organization will mitigate any losses, and how it will recover
- The firm's written guidance and periodic training to employees concerning information security risks and responsibilities
- Policies and procedures if customers have online access to their information
- Whether the firm updated its written supervisory procedures to detect identity theft flags for rules that became effective in 2013 under 17 CFR 248
- Results of the last performed penetration tests and vulnerability scans

Cost to the Economy

As evident above, U.S. regulators are putting cybersecurity in the spotlight. While firms are always at risk of a cyber breach, the regulators are taking measures to ensure that loss of consumer financial and personal data is minimized. The cost that firms will be taking on to enhance cybersecurity measures will be substantial, but they will attempt to offset a large cost that some firms are already encountering.

A MacAfee sponsored research report conducted in 2013, "The Economic Impact of Cybercrime and Cyber Espionage," indicated that worldwide cyber attacks cost at least $300 billion per annum. This research comes on the heels of a U.K. study, performed by the Office of Cybersecurity and Information Assurance, which noted that cyber attacks cost the U.K. alone approximately $40 billion a year.

Companies that have been shaken by cyber theft face not only reputational risk and financial loss, but also the derivative effect of their customers' social security numbers, birthdates, emails, and street addresses being used later by criminals. As an example, the following represent large companies that have recently experienced a theft of their customer information:

- **Target -** Nearly 40 million customers' credit and debit card numbers were stolen in the midst of holiday shopping rush. This breach may result in upwards of $3.6 billion dollars of fines, penalties, and class action suits
- **Adobe** - Reported that 3 million customers' credit card information, 38 million customers' IDs, and source code for Adobe products were stolen. The financial, reputational, and intellectual property losses have not yet been determined
- **New York Presbyterian Hospital, Columbia University, and Triple-S Salud, Inc. -** Had personal medical records stolen. So far the accumulated fines are in excess of $10 million
- **Neiman Marcus** – Notified over 1 million customers that their credit card information was stolen. Neiman Marcus has already accumulated over $4 million in legal bills
- **Heartland Payment Systems** - Lost 100 million records in 2009. This credit card processor has paid about $140 million in fines and settlements so far
- **Citibank -** Approximately 360,000 customer accounts were compromised
- **LivingSocial** - 50 million user emails and passwords were stolen

Cost to your company

The Ponemon Institute issued a "cost of data breach study" in May 2014 that indicated that the average security breach costs an affected company approximately $5.85 million. However, the damage to your firm's reputation, management distraction, and loss of current and future business might be felt for quite some time. Once your customers or investors lose confidence in your firm, the effort to bring them back in the fold will be huge. Frank Murphy, Managing Director of TBG Security Inc. states, "A company's most sensitive information may be on a spreadsheet which may not be subject to the same security protocol as other system applications. The secret sauce is therefore vulnerable to thieves."

Recognizing the potential economic consequences of this continuing trend, we have seen governments sharing more information and a convergence of guidelines and promulgated rules for regulated and unregulated firms to follow. Emphasizing this point are the guidelines issued by the White House and rules issued by the SEC and FINRA have issued rules. These rules and guidelines should be followed.

What your organization should be doing now

- Determine what information your organization needs to protect. This can take the form of customer/investor, firm, and non-public information
- Perform a risk assessment of how your organization manages its cyber risk. This should include documenting your organization's unique vulnerabilities, risk appetite (what type of impact each event might cause), and how your organization controls these cyber threats
- Map out your organization's network connections and data flow. The access points that manage your data will be the most vulnerable points of an unauthorized breach.
- Manage these threats by ensuring good controls. These controls need to be monitored on a periodic basis through vulnerability and penetration testing
- Where does this information reside? Using a "cloud" or third-party provider that maintains your proprietary information will not necessarily provide 100% protection. Certainly, using a reputable third-party vendor may give you some comfort, but you should still ensure that the third-party will provide you with evidence that they have sufficient security over your data
- Your firm should develop and implement policies and procedures that are designed to prevent and detect cybersecurity events. Further, policies and procedures should include the processes that should be triggered if a cyber breach occurs. Policies and procedures should be updated periodically when your technology architecture changes or when new regulations are enacted. Cybersecurity policies should dovetail into your organization's overall IT security and business continuity policies and procedures
- The awareness and adherence with all policies and procedures must be strongly supported by individuals at the highest level of your organization. Your organization should properly communicate its cybersecurity program to employees
- Hire or appoint an individual in your firm who will be responsible for ensuring that all cybersecurity-related issues are addressed in a timely manner
- Your organization's mitigation of cybersecurity risk, in large part, is the responsibility of all the employees within the firm who have access to applications and data. Your organization should train employees to ensure cybersecurity awareness. Further, your organization should know which employees might have access to sensitive information
- Ensure that sensitive data is always encrypted or properly masked
- Consider reviewing your insurance policy to

include cybersecurity coverage

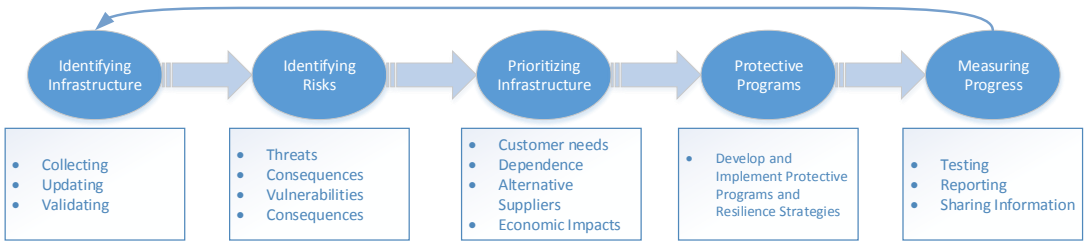
How can we help your organization?

Our firm has deep experience in IT security, operational risk management, and corporate governance. Depending on your organization's needs, we can provide a complete turnkey solution or assist your staff where we can add the most value. We will:

- Identify the cyber risks in your organization
- Perform an assessment to determine the vulnerabilities and associated controls as they relate to your organization
- Assist in remediating any data vulnerabilities
- Assist your organization in testing the controls
- Review data control over your organization's desktops and mobile devices
- Review third party contracts
- Work with your team to map your network
- Draft policies and procedures unique to your organization
- Educate and train your employees about the significance of the organizations data

Appendix A

Vulnerability Assessment Methodology



About Navint Partners

Navint is a different kind of management consulting firm, excelling in large scale business process change. With offices in New York, Chicago, Boston, Pittsburgh, Philadelphia and Rochester, Navint's consultants specialize in managing the alignment of people, processes and technology when organizations face operational restructuring and IT transformation. A unique blend of experience and innovative thinking allows Navint consultants to address clients' business challenges in imaginative ways. http://www.navint.com.

Larry Wagner, Principal, Navint Partners, LLC
Contact information; Lwagner@navint.com; Phone (888) 607-6575 x 737.