WHITE PAPER

Cyber Security in Financial Services: A Complex Threat Requiring a Comprehensive Strategy

An Osterman Research White Paper

Published April 2017

wombat® security technologies

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 206 683 5683 • info@ostermanresearch.com
www.ostermanresearch.com • @mosterman

EXECUTIVE SUMMARY

Financial professionals and financial services firms – broker-dealers, investment advisors, hedge fund managers and others – face unprecedented challenges and risks when it comes to cyber security. Unfortunately, many of them are quite unprepared to address these challenges:

- More regulation and increased scrutiny
- Increased risk from new threats and more sophisticated threats, and
- Greater risk as access to financial information and electronic records is increasingly moving online and accessed via mobile and other devices.

For example, the *Verizon Data Breach Investigations Report* found that 93 percent of compromises take no more than a few minutes to infect machines, but these breaches are taking longer to detect. Moreover, the vast majority of cyber criminals attack systems for purely financial reasons – and the proportion of attacks motivated by financial gain is on the increase, as evidenced by the explosion of ransomware that has resulted in the loss of billions of dollars. Underscoring the depth of the problem, 100 percent of the Registered Investment Adviser firm leaders surveyed by their trade group said that they were either moderately or very concerned about cyber security over the next 24 months[i].

In addition to the attacks themselves, financial firms risk significant penalties, as well. For example, in December 2016, twelve firms were fined $14.4 million[ii] by the Financial Industry Regulatory Authority (FINRA) for their failure to retain records in a write once-read many (WORM) format. While this fine was ostensibly a failure of these firms' archiving obligations, it is just as much an issue for the security of these records. The multimillion-dollar fine is in line with FINRA's broader crackdown on cyber security lapses, which it communicated earlier in 2016 as a regulatory and examination priority.

This white paper will offer a multi-dimensional view of the complex cyber security landscape that financial firms and professionals face, as well as some best practices to reduce risk, maintain compliance, mitigate security threats, and ideally avoid fines, bad press, loss of corporate reputation and loss of revenue.

KEY TAKEAWAYS

- Both financial organizations and users are moving to a cloud-based world filled with mobile devices and online access. In addition, financial organizations and banks are pursuing digital strategies and utilizing newer channels for communications like email, social media and texts to reach today's consumer and gain, or simply maintain, their market share. These trends will only build momentum in our global economy, particularly as new, late adopters in developed nations and new users in developing nations go online with access through smartphones.
- IT decision makers and professionals in financial services should be highly concerned about cyber security problems like insider threats, breaches of unencrypted data, phishing, malware infiltration, ransomware, identity theft and Business Email Compromise (BEC). Most organizations have been the victim of these types of attacks and exploits, as well as others, during the last 12 months.
- Cyber security solutions in place today are somewhat effective, but a significant proportion of decision makers report that their cyber problems are getting worse over time. The majority of decision makers report that the cyber security capabilities that organizations have deployed to combat these threats are not highly effective[iii].

Cyber security solutions in place today are somewhat effective, but a significant proportion of decision makers report that their cyber problems are getting worse over time.

- Users continue to be the weak link in most organizations' cyber security infrastructure because they have not been adequately trained to deal with targeted attacks via email like phishing, spearphishing and CEO Fraud/BEC attempts.

- Cyber criminals are becoming more sophisticated, better funded and are outpacing spending on new cyber security solutions and security awareness training. Consequently, the medium-term trend is that the problems associated with these targeted attacks are getting worse, especially for businesses, governments and wealthier organizations like financial firms.

- However, there are a number of steps that organizations can and must take to significantly improve their cyber security defenses. These will dramatically reduce the chances of falling victim to these attacks and help organizations to comply with regulatory standards.

ABOUT THIS WHITE PAPER

This white paper focuses on financial professionals working in the investments and securities area, which employed 920,700 people in the United States at the end of 2015. However, the trends, issues, and best practices discussed in this paper apply to the millions of people who work in the financial services industry across the globe. This paper was sponsored by Wombat Security Technologies – information about the company is offered at the end of the paper.

THE REGULATORY LANDSCAPE FOR FINANCIAL SERVICES FIRMS

General compliance and regulations governing financial professionals, as well as specific cyber security initiatives and examinations and risks of fines, require a robust cyber security strategy.

RECENT CASES AND FINES

As noted earlier, in December 2016, twelve firms (First Clearing, LLC; Georgeson Securities Corporation; LPL Financial LLC; PNC Capital Markets LLC; RBC Capital Markets LLC; RBC Capital Markets Arbitrage S.A.; RBS Securities, Inc.; SunTrust Robinson Humphrey, Inc.; Wells Fargo Advisers, LLC; Wells Fargo Advisors Financial Network, LLC; Wells Fargo Prime Services, LLC; and Wells Fargo Securities, LLC) were fined $14.4 million dollars by FINRA for their supervisory and procedural deficiencies with regard to protecting the integrity and security of customer financial records. The multimillion-dollar fine is in line with FINRA's broader crackdown on cyber security lapses, which it communicated earlier in 2016 as a regulatory and examination priority. However, there have been other, cyber security-related fines from FINRA in the recent past:

- In November 2016, a subsidiary of Lincoln Financial Group, Lincoln Financial Securities, was fined $650,000 by FINRA for its failure to resolve security problems arising from a 2012 data breach. This followed a February 2011 fine of $450,000 on Lincoln Financial Securities and a fine of $150,000 on Lincoln Financial Advisors for cyber security violations[iv].

- In September 2015, investment adviser R. T. Jones Capital Equities Management was fined $75,000 for storing customers' personally identifiable information (PII) on a third-party's hosted web server that was infiltrated by a Chinese hacker[v].

- In May 2015, financial services firm Sterne Agee & Leach was fined $225,000 for its loss of a laptop computer that contained unencrypted personal and financial information on more than 350,000 of its customers[vi].

- In July 2014, broker-dealer LavaFlow, Inc. was fined $2.85 million for its failure to implement safeguards to protect the confidential information of its subscribers. Moreover, an affiliated company, Lava Trading, Inc., was penalized $1.8 million in earnings paid $350,000 in interest payments[vii].

We have provided some of the key cyber security and data protection regulations governing financial services firms in the United States and elsewhere in the Appendix to this white paper.

TRENDS IN FINANCIAL SERVICES HAVE INCREASED THE THREATS

Cyber security is acknowledged as an issue for investors, consumers, regulators and employees in the financial services industry all the way up to boards of directors. However, there are certain trends that have actually increased the threat to doing business and protecting client data and funds.

ONLINE BANKING AND CLOUD SOLUTIONS

Both financial professionals and consumers have adopted cloud-based solutions – access to these solutions online and adoption of online banking have increased dramatically over the past 10 years. A global survey released in 2015 by the Cloud Security Alliance showed that:

- 32 percent of financial institutions had a cloud software strategy in place, and
- 61 percent were developing one.

This growing interest is explained in part by a 2015 report from Forrester Research that reported that banks need to use SaaS to accelerate their digital business transformation.

It is important to note that risks are not limited simply to outsiders gaining access to data, accounts or putting themselves in the stream of a financial process. For example, financial organizations that do not build and bolster insider threat detection programs likely face a new wave of successful attacks that can be equally or even more damaging. Moreover, as organizations move to cloud-based/SaaS applications, they have inherently less visibility into potential security breaches, such as phishing attacks. This expands firms' audit scope if they must validate the security practices for multiple cloud vendors and subcontractors.

DIGITAL COMMUNICATIONS, USE OF NEW COMMUNICATIONS CHANNELS AND BYOD

The days of executing financial transactions solely over the phone with a trusted advisor or in person at a branch office are long gone. Communications options have multiplied in recent decades to include such channels as email, social media, collaboration tools, texting, and even unsupported apps. Many financial professionals simply could not respond to client needs without use of many of these technologies on a daily basis.

For example, a Pew Research study in 2013 showed that 51 percent of U.S. adults, or 61 percent of Internet users, bank online. Thirty-two percent of US adults, or 35 percent of mobile phone owners, bank using their mobile phones. Pew Research in 2015 also shared that 68 percent of American adults now own a smartphone and 77 percent of these smartphone owners have downloaded apps in the past (other than the ones that came pre-installed on their phone). Moreover, one can simply check the news to see the rising trend of malware and rogue or counterfeit apps on smartphones.

Bring Your Own Device (BYOD) has skyrocketed in recent years, as has shadow IT, the phenomenon of employees implementing cloud applications, mobile apps and

other IT tools independently of their employer's formal IT operation. A Cisco study of CIOs in 2015 study found that CIOs estimated there were 51 cloud services running within their organizations, when in fact, the number is closer to 730.

Companies that manage these trends effectively will create a competitive advantage through customer loyalty and insight. Companies that experience a breach or fail to respond to a security issue face risks to brand image and loss of goodwill with customers. In some cases, executives and the financial professionals themselves could lose their jobs and damage their own careers.

FPA SURVEY SHOWS MUCH WORK TO DO AROUND CYBER SECURITY

Research shared in 2016 by the Financial Planning Association's (FPA) Research and Practice Institute found that only 29 percent of 1,015 financial advisors it polled considered themselves "fully prepared to manage and mitigate the risks associated with cyber security." Moreover, roughly 70 percent of advisor respondents said their clients were at least somewhat aware of the risks associated with data security, yet only 44 percent of advisors completely agreed that they fully understood cyber security issues and risks.

Firms in the FPA survey had a mixed bag of documented policies and procedures in place to deal with cyber security issues:

- Governance and risk assessment: 57 percent of organizations
- Access rights and controls: 59 percent
- Data loss prevention: 58 percent
- Training: 51 percent
- Vendor management: 43 percent
- Incident response: 43 percent

The trends represented by these data points are not isolated to only these types of professionals, but rather illustrate that the firms, clients, and financial professionals and their support teams still have a lot of work to do in the cyber security arena.

PROBLEMS WITH THE DISTRIBUTION CHANNELS AND INDEPENDENT FINANCIAL FIRMS

While financial firms can, to some degree, proactively address risks associated with these new channels using training and practices with their own employees, challenges increase for independent businesses and third-party distributors.

A North American Securities Administrators Association study in 2014 found that most small and midsize state-registered financial advisors have tech or cyber security policies in place, but that only 4.1 percent of the participants were aware that they had suffered a cyber security incident. The study found that 85 percent of these advisors do not use mobile device management that could indicate that the advisors' ability to protect data on lost or stolen smartphones is lacking. While 76 percent of the advisors said that they utilize online or remote backup solutions, experts say that the vast majority of these are not encrypted, subjecting the firm to data loss.

TRAINED CYBER SECURITY PROFESSIONAL ARE IN HIGH DEMAND

While the regulations are multiplying and threats seem to be increasing exponentially, trained cyber security professionals are scarce and in high demand. Financial firms may have the processes and tools to fight against cyber criminals, but may lack the people to maintain the necessary defenses because they have overlooked the technical skills of their staff members. Moreover, program management standards often do not exist at many firms and there is only minimal analysis and tool standardization in the industry, leading to a number of different approaches toward security. In addition, there is insufficient collaboration within the financial community,

While the regulations are multi-plying and threats seem to be increasing exponentially, trained cyber security professionals are scarce and in high demand…

so it is difficult to have consistent levels of protection and universally applicable lessons learned.

KEY CYBER SECURITY RISKS FOR FINANCIAL PROFESSIONALS AND ORGANIZATIONS

Cyber security risks for financial firms and professionals include, but are not limited to, the following types of threats:

- **Phishing and spearphishing**
  The fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information. A common financial services example is a message would try to lure the recipient into giving their personal information by pretending that their bank or email service provider is updating its web site and that they must click on the link in the email to verify account information and password details.

- **Identity theft**
  The fraudulent acquisition and use of a person's private identifying information, usually for financial gain. A common example in financial services is to gain personal information with the purpose of draining an account. Victims are often smaller organizations, such as churches and school districts, that often lack sophisticated IT and/or security expertise.

- **Data breaches and loss of customer data**
  An incident in which sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), trade secrets or intellectual property. It is important to note that a data breach can occur – and the party guilty of the breach can be fined (as in the case of Sterne Agee & Leach noted earlier) – even if the data was not used for malicious purposes.

- **CEO Fraud/Business Email Compromise (BEC)/Whaling**
  Business Email Compromise (BEC) is a sophisticated scam that targets businesses often working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The email appears to come from an executive directing a senior employee to make a transfer to a trusted recipient, but the funds are actually sent directly to a criminal organization.

- **Ransomware**
  Malicious code designed to block access to a computer system, typically by encrypting the victim's files, until a sum of money is paid. Its roots come from targeting individual users, but as criminals have become more sophisticated it has increasingly targeted businesses and financial institutions.

- **Insider threats and need for employee vigilance**
  A malicious threat to an organization that comes from people within an organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems. Insider-outsider collusion can occur when an employee shares or sells information with an outside party and then exploits it for financial gain. Stolen credentials are also a serious threat, permitting an external bad actor to become an "insider".

- **Users are a weak link in the security infrastructure**
  Users are an easy target for delivering a malicious file or request because their behavior is predictable, many users are not careful, most are not well trained, and because many of them are not sufficiently skeptical about what they receive or interact with on the Internet. Criminals mimic common communications

content and vectors, such as email, to which users are already responding. Homegrown security training is almost universally inadequate and many organizations do not provide the infrastructure to support better, user-focused security.

- **Malware and viruses**
  Malicious software that is designed to infiltrate and damage computers without the user's consent. This general term covers all the different types of threats to computer safety, such as viruses, spyware, worms, Trojans, and rootkits. These programs began as simple disruptions to individual users, but have evolved to deliver sophisticated programs, often without being detected, that compromise systems for the purpose of financial gain or delivering ransomware.

- **Cyber criminals are shifting their focus by "cutting out the middleman"**
  One trend is for a reduced emphasis on stealing content to be sold on the open market. In a sense, past cyber crime has almost been too successful and prices of stolen credit cards, credentials, etc. on the open market have dropped, so that the economic motive is to go for the funds directly, such as through ransomware and BEC attacks.

- **Greater emphasis on stealing funds directly**
  Payment systems, ATMs and accounts are under attack directly. Cyber criminals are increasingly looking to get into the middle of a financial process and siphon off funds directly.

- **Social media**
  People who use social media often consider themselves part of a "tribe" and so tend to trust one another, often inadvertently clicking on links that can introduce malware into the organization. Social media can also be used to craft effective spearphishing emails.

CYBER SECURITY PROBLEMS ARE GETTING WORSE

Compounding the problem of ineffective cyber security solutions and inadequate training is that phishing, spearphishing, CEO Fraud/BEC and ransomware are becoming more common threats each year; while data protection and user privacy obligations are becoming more onerous. For example:

- The Anti-Phishing Working Group reports that the number of unique phishing sites it detected grew from 0.39 million in 2014 to 0.79 million in 2015, a 103 percent increase, to 1.49 million in 2016, an 89 percent increase[viii].

- The FBI reported that identified, exposed losses from CEO Fraud/BEC increased by 1,300 percent from January 2015 to June 2016[ix].

- The FBI reported that ransomware victims paid $24 million in ransom in 2015, but $209 million in just the first quarter of 2016 and was on-pace to be a $1 billion problem for all of 2016, an increase of more than 4,000 percent[x].

- The Identify Theft Resource Center reported that the number of data breaches increased from 614 in 2013 to 783 in 2014, a 28 percent increase, and dropped only slightly to 781 in 2015.

The fundamental challenge for decision makers is to improve data protection in response to these growing threats without violating privacy in the process – an increasingly difficult balance.

The fundamental challenge for decision makers is to improve data protection… without violating privacy in the process.

TWELVE BEST PRACTICES FOR CYBER SECURITY DEFENSES

Executives, professionals, board of directors and front-line employees must all appreciate the risks that financial firms face and recognize that the number of opportunities to steal data and funds is increasing.

Decision makers must acknowledge that criminal strategies that utilize phishing, spearphishing, CEO Fraud/BEC and ransomware are not going away anytime soon. Decision makers should make it a high priority to address them in a comprehensive fashion. Implementing the right cyber security infrastructure is a good start, supplemented by the best practices outlined below.

DEVELOP A CYBER SECURITY PROGRAM BACKED BY C-SUITE AND BOARD OF DIRECTORS

Cyber security requires a strategy at the firm level and the appropriate level of commitment and funding that includes, but extends beyond, the necessary tools. The correct "tone from the top", including the C-suite and board of directors, goes a long way towards pushing out the strategy throughout the firm.

The strategy should incorporate both enterprise tools and "Bring Your Own" (BYO) capabilities. It should also encompass best practices around corporate and personally managed tools, devices, and data repositories, including:

1. **Periodically complete a comprehensive audit of tools, training, and practices**
   Organizations should conduct a thorough audit of their current cyber security infrastructure, including their security awareness training regimen, the security solutions they have in place, and the processes they have implemented to remediate security incidents.

   Organizations should also engage in their own, internal testing of readiness to respond to attacks. This is an essential element in identifying the deficiencies that may (and probably do) exist, and it can be used to prioritize spending to address problems.

2. **Establish policies**
   It is important to develop policies for all of the email, Web, collaboration, social media, mobile and other solutions that IT departments have deployed or that are allowed for use as part of BYO/"Shadow IT" practices. As a result, Osterman Research recommends that a key step should be the development of detailed and thorough policies focused on the tools that are or probably will be used in the future. Policies should focus on legal, regulatory and other obligations to encrypt emails if they contain sensitive or confidential data; monitor all communication for malware that is sent to blogs, social media, and other venues; and control the use of personal devices that access corporate systems that contain business content.

   Policies on their own will not provide total cyber security, but they can be useful in limiting the number of solutions that employees use when accessing corporate systems. These limitations can be helpful in reducing the number of ingress points for ransomware, other forms of malware, phishing and spearphishing attempts, and other content that might pose a cyber security risk.

3. **Employee training with additional training for senior executives to deal with spearphishing and CEO Fraud/BEC**
   A solid security awareness training program will help users to make better decisions about the emails on which they act, and how they use the internet, social media, and other channels. While security awareness training alone will not completely address an organization's cyber security risk, it will bolster users

as the "first line of defense" and make the organization less susceptible to attacks.

Senior executives should have additional training to deal with spearphishing and CEO Fraud/BEC, since they are higher value targets to cyber criminals and the consequences of their failure can be dramatically greater.

4. **Proactively protect sensitive data**
   Because virtually all damaging data breaches have involved unencrypted data, organizations should protect sensitive and confidential data through encryption, tokenization or other techniques that will render breached data useless. Doing so will almost entirely nullify a breached organization's notification obligations, since almost all regulatory obligations do not obligate an organization to notify affected parties if encrypted data was breached.

5. **Limit exposure of data to third parties**
   The more that an organization can do to limit exposure of their data to third parties, the easier their compliance auditing will be. This is true for any organization that possesses and manages sensitive or confidential information, but especially so for financial services firms.

6. **Employee testing**
   Employees should be tested on a regular basis to determine if their security awareness training has been effective, and to identify those employees that might need additional training.

7. **Behavioral analytics**
   Analyzing the behavior of users is an increasingly important best practice because it can provide much deeper insight into user behavior than traditional metrics have afforded. The use of behavioral analytics can yield important insights into not only how users have acted, but also why they act as they do and how they will act in the future. This can provide decision makers with more information about how threats may impact their organizations and how they can become more proactive about dealing with emerging threats.

8. **Good password management**
   Employees should use passwords that match the sensitivity and risk associated with the corporate assets they are accessing. These passwords should be changed on an enforced schedule established by IT.

9. **Create backchannels**
   Create communication "backchannels" for staff members that will be involved with corporate finances or sensitive information. For example, if a CEO sends a request to her CFO to transfer funds to an established vendor, the CFO should have a means of verifying the authenticity of the CEO's request before initiating the transfer, such as texting or calling the CEO's smartphone. In many cases, cyber criminals will have infiltrated a corporate network months before a CEO Fraud/BEC attempt for the purpose of studying the company's wire transfer patterns and senior executives' travel schedules, the goal of which is to initiate a transfer request when the supposed requestor of the transfer is out of the office and harder to contact.

10. **Ensure analyst staff are current in their skill sets**
    Analyst staff must have adequate certifications to ensure the currency of their skills sets, requiring executive/C-suite sponsorship to ensure a high level of talent in the organization. Many organizations do not adequately appreciate the broad spectrum of skill sets and relevant knowledge that are required to ensure that controls are in place and working properly.

11. **Implement distributed, centrally managed security**
    For organizations that are going direct-to-cloud for distributed locations, such as

Create communication "backchannels" for staff members that will be involved with corporate finances or sensitive information.

satellite offices or employees who are working remotely, and that are not backhauling all traffic through a headquarters location for security scanning, it is essential to implement security that is distributed, yet centrally managed for these remote locations that can also monitor employee-owned/managed devices.

12. **Apply updates**
    Employees should be reminded and required to keep software and operating systems up-to-date to reduce the potential for a known exploit to infect a system with malware. IT can help through management and enforcement on behalf of users. This includes keeping policies synchronized across all locations quickly and reliably so that remote locations are no more at risk of security breaches and the like than is a headquarters location.

SUMMARY AND CONCLUSION

Cyber security challenges both firms and professionals to develop and be vigilant about implementing a firm-wide security strategy. The stakes have been raised as access to financial information and electronic records is increasingly moving online and accessed via mobile and other devices.

In response to the escalation of threats and impact of breaches, more regulations and examinations have been introduced with teeth behind them.

This white paper has attempted to share a multi-dimensional view of the complex cyber security landscape that financial firms and professionals face, as well as some best practices, tools, and strategies to reduce risk, maintain compliance, and mitigate security threats.

Organizations that work on all of these fronts will strengthen their defenses and take steps to help ensure the long-term future of the organization itself.

SPONSOR OF THIS REPORT

Wombat Security Technologies provides information security awareness and training solutions to help organizations teach their employees secure behavior. Our Continuous Training Methodology takes a 360-degree approach to security education with a continuous cycle of assessment, education, reinforcement, and measurement to maximize learning and strengthen retention. Our customers have experienced up to a 90% reduction in phishing attacks and malware infections when using this four-step approach to security awareness and training.

Our integrated SaaS-based Security Education Platform offers a library of simulated attack tools, broad knowledge assessments, interactive training modules, awareness materials, and comprehensive reporting features; allowing customers to deliver customizable content covering a variety of topical security risks in more than 25 languages. Our security awareness and training solutions are ideal for information security officers and risk managers who want to proactively identify and address end-user susceptibilities, progressively educate end users on relevant threats in their workplace and industry, measure progress and evaluate performance, and create an overall culture of good security habits and safe behavior.

Born from research at Carnegie Mellon University in 2008, Wombat Security has grown into a global leader in security awareness and training with millions of users across North America, Europe, and Asia. Recognized for three consecutive years by Gartner as a leader in the Magic Quadrant for Security Awareness Computer-Based Training Vendors and ranked 144 on Deloitte's Technology Fast 500™, we continue to help Fortune 1000 and Global 2000 customers across the globe in industry segments such as finance and banking, energy, healthcare, technology, higher education, retail and consumer packaged goods to effectively change behavior and reduce risk.

www.wombatsecurity.com
@WombatSecurity
info@wombatsecurity.com
+1 888 687 1337
+1 412 621 1484

To learn more about Wombat Security, visit us at www.wombatsecurity.com.

AUTHORS OF THIS REPORT

BOB HANSON, QUANTUM LEAP MARKETING, INC.

Bob Hanson is the President of consultancy Quantum Leap Marketing Inc., and co-author of *Marketing Power for Financial Advisors, How to Create a Predictable Flow of Your Ideal Prospects*, AuthorHouse, 2014. Bob has interviewed over 1,000 financial planners and advisors and spent much of the last 10 years incorporating winning communications strategies and tools into planning and advisory practices of all types.

He has worked as a product marketing executive for a messaging management provider and produced over 1,000 webinars and online conferences for the financial services, email and IT markets reaching over 100,000 attendees. To request a no-obligation consultation on creating successful communications or events programs, email Bob at bhanson@qlmarketing.com or go to www.qlmarketing.com.

MICHAEL OSTERMAN, OSTERMAN RESEARCH, INC.

Michael Osterman is the principal of Osterman Research, Inc., founded in 2001. Since that time, the company has become one of the leading analyst firms in the messaging and collaboration space, providing research, analysis, white papers and other services to companies like Microsoft, IBM, Google, EMC, Symantec, Hewlett Packard and many others.

Prior to founding Osterman Research, Michael was the Vice President of Market Research at Creative Networks, a leading market research and consulting firm focused on the messaging and directory markets. Michael has also held positions with the SRI International Business Intelligence Center, Ryan Hankin Kent, ElectroniCast and Gnostic Concepts. His background includes research and analysis of various markets, including computer-aided software engineering, data communications, telecommunications, and fiber optic components.

APPENDIX

SEC AND OTHER COMPLIANCE REQUIREMENTS

The US Securities and Exchange Commission (SEC) views cyber security and a firm's compliance obligations under the federal securities laws as closely connected. Cyber security threats can impact a firm's ability to comply with certain federal securities laws and, as a result, firms should examine their ability to respond to cyber security threats in that context. For example:

- **Privacy of Consumer Financial Information (Regulation S-P)**[xi]
  Rule 30 of Regulation S-P includes, "Every broker, dealer, and investment company, and every investment adviser registered with the Commission must adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information. These written policies and procedures must be reasonably designed to: 1) Insure the security and confidentiality of customer records and information; 2) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and 3) Protect against any unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."

- **Regulation Systems Compliance and Integrity (Regulation SCI)**[xii]
  The goal of this rule is "to strengthen the technology infrastructure of the U.S. securities markets. Specifically, the rules are designed to reduce the occurrence of systems issues; improve resiliency when systems problems do occur; [and]

enhance the Commission's oversight and enforcement of securities market technology infrastructure."

- **General Rules and Regulations, Security Exchange Act of 1934 (Title 17, Chapter II, Part 240, §240.13n-6 Automated Systems)**[xiii]
  "Every security-based swap data repository, with respect to those systems that support or are integrally related to the performance of its activities, shall establish, maintain, and enforce written policies and procedures reasonably designed to ensure that its systems provide adequate levels of capacity, integrity, resiliency, availability, and security."

- **Identity Theft Red Flags Rule (Regulation S-ID)**[xiv]
  Section 248.201 requires "each financial institution and creditor that offers or maintains one or more covered accounts, as defined in §248.201(b)(3), to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account."

- **The Securities Exchange Act of 1934**
  This Act requires firms to preserve their electronically stored records in a non-rewritable, non-erasable format. While ostensibly focused on archival of customer records, the retention of records in a tamper-proof format is as much about security as it is archival of this content.

In April 2015, the SEC Division of Investment Management updated guidance identifying the cyber security of registered investment companies and registered investment advisers as a critical issue, and detailed measures that may be considered to address cyber security risks. In many ways, the update focuses on the same key issues that other regulators have found important for addressing cyber security risk: risk assessment, effective governance, creating an incident response plan, participating in cyber threat information sharing bodies, assessing the risk posed by third-party vendors and considering cyber insurance.

The April 2015 update provides a number of specific measures firms may consider implementing to protect confidential information, including information about fund investors and advisory clients, from a cyber attack. The update recommends that firms:

- Conduct periodic assessments to identify cyber security threats and areas of vulnerability in order to prioritize and mitigate risk.

- Create a strategy designed to prevent, detect and respond to cyber security threats.

- Adopt written policies and procedures to implement the strategy.

GENERAL DATA PROTECTION REGULATION

Protecting personal data has been an important issue in the European Union (EU) for more than 20 years, and the recently ratified General Data Protection Regulation (GDPR) takes data protection to an entirely new level. The regulation was published officially in early May 2016, and was effective immediately, with implementation required by all affected organizations by May 25, 2018. The GDPR is among the most serious issues with which organizations will have to contend given the enormous penalties associated with non-compliance: up to €20 million or four percent of the offender's annual revenue[xv].

In addition to a new set of legal requirements that require both organizational and technological responses, the GDPR is applicable to almost every organization around the world that collects or processes data on residents living within the EU, including permanent residents, visitors and expatriates. Compliance is based on the geographical location of the individuals about whom an organization holds personal

data, not the domicile of registration for the organization. In other words, a physical presence in the EU is not a prerequisite for being subject to the GDPR, only the collection and/or processing of an EU resident.

While a successful malware infiltration can render computers unusable – a costly annoyance and interruption that most organizations will want to avoid – a more serious concern under GDPR is the potential for any threat that can harvest credentials for user and administrator accounts, thereby breaching an organization's data protection infrastructure. These harvested credentials can then be used to access data sources across the organization, both on-premises and in the cloud, including those containing personal and other sensitive data. Preventing a malware infection in the first place requires a combination of anti-malware software/services and advanced threat protection. These services need to become commonplace so that every attachment or link in an email, as well as every link on a web page, can be checked for malware.

Maintaining data protection through technology is essential for any organization that wants to become GDPR-compliant in order to reduce the likelihood of data breaches, among other implications. Additionally, highlighting dangerous or compromised URLs or attachments helps educate the user population about the security risks facing the modern organization and should be part of a thorough and regular training plan for all users. Employees should receive thorough training about the importance of GDPR compliance, including identifying and avoiding malware, phishing and other threats that could lead to non-compliance with the regulation.

Moreover, organizations must show that encrypting and tokenizing with format-preserving technologies that preserves the context, logic, relationships and meaning of content will allow data to be portable and will neutralize the impact of malware. Finally, while malware can create havoc, organizations will also need to protect against malware-less attacks that use trickery to impersonate a trusted or senior-level executive in order to gain access to sensitive information.

The GDPR requires that organizations embrace data protection "by design and by default," which means data protection considerations should be an always-on approach, not an afterthought at the tail end of a development job or selection process. Approaches like data encryption, classification and pseudonymization should, therefore, become initial discussion and design points. Likewise, technologies that proactively test for security vulnerabilities during development and deployment should be evaluated as a way of operationalizing a data protection-by-design mindset and approach.

FINRA AND SEC EXAMINATION PRIORITY

Cyber security has been identified as an examination priority for regulating bodies at the state level, as well as FINRA and the SEC. The position of these organizations is that we all face the same challenges and the goal is to protect consumers from the constant onslaught of insider threats and the scams and bad actors that perpetrate them:

- The SEC has made cyber security a major initiative, notably with the 2014 Cyber Security Examination Sweep that included targeted exams of more than 100 broker/dealers and investment advisers that assessed firms' overall preparedness to deal with cyber attacks.

- The SEC's Office of Compliance Inspections and Examinations (OCIE) noted in its 2015 Cybersecurity Examination Initiative[xvi] that it would focus on six key areas in the context of cybersecurity:

    - Governance and Risk Assessment
    - Access Rights and Controls
    - Data Loss Prevention
    - Vendor Management

  - Training
  - Incident Response

- Similarly, the SEC's Division of Investment Management issued a Guidance Update in April 2015[xvii] noting the critical nature of cyber security threats and offering similar guidance to the OCIE. In its Examination Priorities for 2016, the SEC announced that it would continue to focus on cyber security as a high-priority, market-wide risk.

- As it pertains to cyber security, FINRA's 2016 CyberSecurity Conference highlighted the use of publicly available frameworks, particularly NIST or ISO2 7001. Firms are also encouraged to take advantage of the centralized information sharing networks available to them, which can include behavioral analytics capabilities.

- The SEC's examination priorities for 2017[xviii] are focused on three key areas:

  - Protecting retail investors
  - Focusing on senior investors and retirement investments
  - Assessing market-wide risks

  As noted in the SEC's Office of Compliance Inspections and Examinations *Examination Priorities for 2017*, "In 2017, we will continue our initiative to examine for cybersecurity compliance procedures and controls, including testing the implementation of those procedures and controls."

  Moreover, FINRA's *2017 Regulatory and Examination Priorities Letter*[xix] notes that "Cybersecurity threats remain one of the most significant risks many firms face, and in 2017, FINRA will continue to assess firms' programs to mitigate those risks." The Letter goes on to note two significant shortcomings: "cybersecurity controls at branch offices, particularly independent contractor branch offices, tend to be weaker than those at firms' home offices", and "firms have failed to fulfill one or more of their obligations [to] preserve certain records in…WORM format."

THE CYBER SECURITY INFORMATION ACT

The Cyber Security Information Sharing Act (CISA S. 2588 [113th Congress], S. 754 [114th Congress]) is a United States federal law designed to "improve cyber security in the United States through enhanced sharing of information about cyber security threats, and for other purposes."

While the law has met with some controversy because of data privacy concerns, the spirit of the law comes from a need for firms, law enforcement agencies, and governments to share information around threats to help combat the ever-changing risk landscape.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

The Payment Card Industry Data Security Standard (PCI DSS) encompasses a set of requirements for protecting the security of consumers' payment account information. It includes provisions for building and maintaining a secure network, encrypting cardholder data when it is sent over public networks and assigning unique IDs to each individual that has access to cardholder information.

SARBANES-OXLEY ACT OF 2002

The Sarbanes-Oxley Act (SOX) requires all public companies to report their company's internal controls and procedures for financial reporting, and auditors are required to test the internal control structures. Businesses must ensure that employees retain relevant information about the company's financial reporting.

NEW YORK DEPARTMENT OF FINANCIAL SERVICES

The New York Department of Financial Services (NYDFS) implemented Cybersecurity Requirements for Financial Services Companies (CRFSC) effective March 1, 2017 (compliance certification will be required as of February 15, 2018). The State of New York, which regulates about 4,000 banks and insurers, recently published the final guidelines for the CRFSC, the most comprehensive cyber security requirements of any US state. The rules require regulated banks and insurance companies doing business in New York to have state-approved plans in place to deter cyber attacks, and to report actual cyber attacks to the state within 72 hours of when they occur. By August 28, 2017, the entities covered under the CRFSC will need to[xx]:

- "Develop and maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's information systems."
- "Develop and maintain a written cybersecurity policy and incident response plan. The policy also must be based on the Risk Assessment."
- "Designate a qualified individual for overseeing and implementing the cybersecurity program and enforcing cybersecurity policy. The person does not need a CISO title, and a third party can be used."
- "Use qualified personnel (including third party service providers) that maintain sufficient current knowledge and training to manage changing cybersecurity threats and countermeasures."
- "…limit user access privileges, and to periodically review those privileges."
- "….start notifying the NYDFS no later than 72 hours after it determines an act or attempt, successful or unsuccessful, was made to gain unauthorized access to, disrupt or misuse an 'Information System' or the information stored on it."

Companies also must reevaluate and upgrade their security systems annually and the guidelines require that boards of insurance companies or banks certify that the companies are in compliance with the security requirements by February 15, 2018. Regulated entities must begin reporting incidents of cyber security breaches to the state starting on September 1, 2017, in some instances.

A GLOBAL VIEW

Across the globe there are a number of important cyber security-focused regulations, including:

- **United Kingdom**
  The UK's Financial Conduct Authority (FCA) imposes various requirements on the 56,000 financial institutions in the UK. These include the Senior Management Arrangements, Systems and Controls (SYSC) rules (SYSC 3.2.6R and 6.1.1R) that requires the deployment and maintenance of systems designed to detect and mitigate the risks associated with financial crimes; and Principles 2 and 3 of the Principles for Businesses that requires the application of appropriate risk management capabilities that are commensurate with the risk of financial crimes against customer data. The fundamental goal of the FCA is for financial services firms in the UK to implement a "security culture[xxi]" focused on all employees within an organization.

- **European Union**
  The EU's Network and Information Security Directive[xxii] is complementary to the GDPR and focuses on the need to protect critical industries from cyber attack, including the financial services industry. The goal of the NISD, which will take effect in May 2018, will be to require organizations in critical industries to implement appropriate risk management practices and report cyber attack

incidents.

In 2013, the European Central Bank published *Recommendations for the Security of Internet Payments*[xxiii], and in 2014 the European Banking Authority published *Guidelines on the Security of Internet Payments*[xxiv].

- **Germany**
  In July 2015, the German government implemented the Act to Increase the Security of Information Technology Systems[xxv], with the goal to protect German citizens by improving cyber security among critical infrastructure providers, among which are financial services firms, energy companies, healthcare providers, food processors and others.

- **Canada**
  In September 2013, the Canadian Securities Administrators (CSA) published Staff Notice 11-326 Cyber Security, which focused on key cyber security elements, such as security awareness training, conducting third-party vulnerability assessments and security tests, and reviewing control processes regularly. Staff Notice 11-332[xxvi], published in September 2016, updated the CSA's recommendations. The Investment Industry Regulatory Organization of Canada (IIROC) surveyed Canadian financial institutions in June 2016 and in October 2016 issued a confidential "report card" to these firms indicating how well they benchmark against a National Institute of Standards and Technology framework for cyber security best practices[xxvii].

- **Hong Kong**
  The Hong Kong Monetary Authority (HKMA) has implemented the CyberSecurity Fortification Initiative (CFI)[xxviii], the goal of which is to make Hong Kong-based banks better able to fend off cyber attacks. The CFI includes three primary initiatives, including the Cyber Resilience Assessment Framework (which includes risk and maturity assessments, as well as cyber attack simulations against riskier banks), a Professional Development Program, and a Cyber Intelligence Sharing Platform.

- **Group of 7**
  The Group of 7 (G7) – the seven major world economies as determined by the International Monetary Fund – has issued *G7 Fundamental Elements of Cybersecurity for the Financial Sector*[xxix], a set of guidelines designed to help financial institutions in the G7 countries (and, presumably, elsewhere) combat financial industry cyber crime.

REFERENCES

[i] The Investment Adviser Association, and Boston-based research firm Cerulli Associates 2016 Study
[ii] http://www.finra.org/newsroom/2016/finra-fines-12-firms-total-144-million-failing-protect-records-alteration
[iii] Osterman Research survey data, 2016
[iv] http://www.natlawreview.com/article/finra-fines-lincoln-financial-sub-650000-cybersecurity-shortcomings
[v] https://www.sec.gov/news/pressrelease/2015-202.html
[vi] http://www.swlaw.com/blog/data-security/2015/06/19/finra-fines-financial-firm-for-failing-to-encrypt-customer-data-on-lost-laptop/
[vii] http://www.bartonesq.com/broker-dealer-assessed-five-million-dollar-cyber-security-penalty-by-sec/
[viii] Osterman Research extrapolation based on January-September 2016 APWG data
[ix] https://www.ic3.gov/media/2016/160614.aspx
[x] http://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646
[xi] https://www.sec.gov/rules/final/34-42974.htm
[xii] https://www.sec.gov/spotlight/regulation-sci.shtml
[xiii] http://www.ecfr.gov/cgi-bin/text-idx?SID=e77a0b38297f6bb207cbc8cf0fe1e199&mc=true&node=se17.4.240_113n_66&rgn=div8
[xiv] http://www.ecfr.gov/cgi-bin/text-idx?SID=e77a0b38297f6bb207cbc8cf0fe1e199&mc=true&node=pt17.4.248&rgn=div5#sp17.4.248.c
[xv] https://planit.legal/en/gdpr/#art-83
[xvi] https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf
[xvii] https://www.sec.gov/investment/im-guidance-2015-02.pdf
[xviii] https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2017.pdf
[xix] http://www.finra.org/industry/2017-regulatory-and-examination-priorities-letter
[xx] https://www.whitecase.com/publications/article/nys-department-financial-services-cybersecurity-regulation-goes-live-now-what
[xxi] https://www.fca.org.uk/news/speeches/our-approach-cyber-security-financial-services-firms
[xxii] http://itlaw.wikia.com/wiki/Network_and_Information_Security_Directive
[xxiii] http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html
[xxiv] http://www.eba.europa.eu/-/eba-issues-guidelines-to-strengthen-requirements-for-the-security-of-internet-payments-across-the--1
[xxv] https://www.insideprivacy.com/data-security/what-you-need-to-know-about-germanys-cybersecurity-law/
[xxvi] https://www.osc.gov.on.ca/documents/en/Securities-Category1/sn_20160927_11-332-cyber-security.pdf
[xxvii] http://www.iiroc.ca/Documents/2016/8272fe2a-a1a5-4319-9b0c-7739d04ff097_en.pdf
[xxviii] https://www.wavestone.com/en/insight/hong-kong-cybersecurity-program-banking-industry/
[xxix] https://www.treasury.gov/resource-center/international/g7-g20/Documents/G7%20Fundamental%20Elements%20Oct%202016.pdf