NSCP
NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

FOR COMPLIANCE. BY COMPLIANCE.

NSCP Currents

Cybersecurity Special Issue

NSCP
NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

CONFERENCES

NSCP Events: Coming to a city near you!

Registration has opened for NSCP's 2018 Spring Conferences & Regulatory Interchanges

Regulatory Interchange
Dallas, TX
April 17, 2018

Spring Conference & Regulatory Interchange
San Francisco, CA
May 3-4, 2018

Spring Conference & Regulatory Interchange
Chicago IL
June 4-5, 2018

Regulatory Interchange
Boston, MA
December 3, 2018

LEARN MORE

NSCP 30th National Conference in Atlanta GA

Save the Date: October 29-31, 2018

LEARN MORE

NSCP
NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

FOR COMPLIANCE. BY COMPLIANCE.

In This Issue:

Simon Says: The SEC and Cybersecurity 5

Data Breach! What to Know About Where to Go 9

SEC and States are Upping Their Cyber Game, Are You Doing the Same? 12

Office of Compliance Inspections and Examinations Identifies Common Weaknesses in Cybersecurity Compliance 16

Compliance Protocols for Dealing with Current Cybercrimes 19

NSCP
NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

FOR COMPLIANCE. BY COMPLIANCE.

Foreword:

Each year, NSCP takes a moment to look back at the prior year and at the contributions that brought our publication, NSCP Currents to life. In 2017, one endless topic of conversation was Cybersecurity.

At the start of 2017, both the SEC and FINRA communicated their continued focus on organizations' cybersecurity risks, noting that it remained a highly ranked operational risk facing many firms.

In February, several NSCP Representatives participated in a SEC Cybersecurity Roundtable, to share member perspectives on the impacts of regulatory focus on this area.

Overarching themes of this dialog, included how:

- Cybersecurity risks, and mitigation plans, cannot follow a once-size-fits-all approach
- Additional guidance from regulatory authorities would be helpful, as the industry is still working to develop "industry best practices" for the implementation of cybersecurity programs.
- Regulatory pressure and focus has aided many organizations from a governance perspective, grasping the attentions of board and senior management.
- Third party vendor due diligence is not yet a perfect science, and education is needed to aid the unwary
- Firms often grapple with budget allocation between cybersecurity insurance versus cybersecurity testing and consulting services.

At the conclusion of the SEC Cybersecurity Roundtable, NSCP in partnership with ACA Aponix, decided to conduct a Cybersecurity Survey in order to gather additional data. The survey covered firm cybersecurity governance practices including dedicated budget; technical controls; cybersecurity insurance and vendor management. A copy of the Cybersecurity Survey results can be found here.

Additional guidance, Alerts, and Observations were released throughout the year, and NSCP Authors remained dedicated to covering these issues. As we prepare for what 2018 has in store in the face of an eruption of technological advances and disruptions, NSCP has prepared a collection of some of our featured Cybersecurity themed articles within this special edition of NSCP Currents.

Simons Says: The SEC and Cybersecurity

By Timothy M. Simons

Originally published September 2017

In light of the Equifax events, cybersecurity will continue to be a hot topic for the financial services industry.

Let's let the DOL rest for a few moments and talk about cybersecurity.

January 9, 2014 - Examination Priorities for 2014

Although the SEC did refer to cybersecurity in the Examination Priorities for 2013, as "information technology systems," it was 2014 before the SEC identified cybersecurity as such, and an Examination Priority:

> "The staff will focus on market access controls related to, among other things, erroneous orders; the use of technology with a focus on algorithmic and high frequency trading; information leakage and cyber security…"

https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2014.pdf

Cybersecurity was listed as a priority under the broker-dealer section of the Examination Priorities for 2014, but it would also apply to the Investment Adviser / Investment Company area. In fact, just three months later the SEC would tell us that.

April 15, 2014 - OCIE Cybersecurity Initiative

This Risk Alert gave the background proving that the SEC was also including advisers in the cybersecurity pool.

"On March 26, 2014, the SEC sponsored a Cybersecurity Roundtable…to gather information and consider what additional steps the Commission should take to address cyber-threats….As part of this initiative, OCIE will conduct examinations of more than 50 registered broker-dealers and registered investment advisers focused on the following: the entity's 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."

Attached to the Risk Alert was a sample document request that would be used for those examinations, and could be used by those firms not examined, to assess their own level of preparedness.

https://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf

February 3, 2015 - Cybersecurity Examination Sweep Summary

This Risk Alert summarized the examinations of the fifty-seven registered broker-dealers and forty-nine registered investment advisers. "The staff conducted limited testing of the accuracy of the responses and the extent to which firms' policies and procedures were implemented. The examinations did not include reviews of technical sufficiency of the firms' programs." (Emphasis added)

- The vast majority of examined broker-dealers (93%) and advisers (83%) have adopted written information security policies.
- The vast majority of examined firms conduct periodic risk assessments, on a firm-wide basis, to identify cybersecurity threats, vulnerabilities, and potential business consequences.
- Most of the examined firms reported that they have been the subject of a cyber-related incident.

About the Author

Timothy M. Simons is a Senior Managing Member at Focus 1 Associates LLC. He can be reached at tim@focus1associates.com.

- Many examined firms identify best practices through information-sharing networks.
- The vast majority of examined firms report conducting firm-wide inventorying, cataloguing, or mapping of their technology resources.
- The examined firms' cybersecurity risk policies relating to vendors and business partners revealed varying findings.
- Most of the examined firms make use of encryption in some form.
- Many examined firms provide their clients with suggestions for protecting their sensitive information.
- The designation of a Chief Information Security Officer ("CISO") varied by the examined firms' business model.
- Use of cybersecurity insurance revealed varying findings among the examined firms. Over half of the broker-dealers maintain insurance for cybersecurity incidents, but less than a quarter of advisers do.

https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf

April, 2015 - Division of Investment Management Guidance Update on Cybersecurity

This was not a Risk Alert, but note that in the Division of Investment Management are the folks that write the IA/IC Rules. The Guidance Update provided three measures that funds and advisers may consider:

- Conduct a periodic assessment of:
    1) the nature, sensitivity and location of information that the firm collects, processes and/or stores, and the technology systems it uses;
    2) internal and external cybersecurity threats to and vulnerabilities of the firm's information and technology systems;
    3) security controls and processes currently in place;
    4) the impact should the information or technology systems become compromised; and
    5) the effectiveness of the governance structure for the management of cybersecurity risk.

- Create a strategy that is designed to prevent, detect and respond to cybersecurity threats. Such a strategy could include:
    1) controlling access to various systems and data via management of user credentials, authentication and authorization methods, and other means, and system hardening;
    2) data encryption;
    3) protecting against the loss or exfiltration of sensitive data by restricting the use of removable storage media and deploying software that monitors technology systems for unauthorized intrusions;
    4) data backup and retrieval; and
    5) the development of an incident response plan.

- Implement the strategy through written policies and procedures and training that provide guidance to officers and employees concerning applicable threats and measures to prevent, detect and respond to such threats, and that monitor compliance with cybersecurity policies and procedures.

https://www.sec.gov/investment/im-guidance-2015-02.pdf

September 15, 2015 - OCIE's 2015 Cybersecurity Examination Initiative

This Risk Alert identified the areas of focus for the second round of cybersecurity examinations, involving more testing to assess implementation of procedures and controls, focusing on:

- Governance and Risk Assessment
    1) cybersecurity governance and risk assessment processes relative to the key areas of focus discussed below.
    2) periodic evaluation of cybersecurity risks and whether their controls and risk assessment processes are tailored to their business.
    3) the level of communication to, and involvement of, senior management and boards of directors.

- Access Rights and Controls:
    1) controls to prevent unauthorized access to systems or information, such as multifactor authentication or

updating access rights based on personnel or system changes.
2) control access to various systems and data via management of user credentials, authentication, and authorization methods.
3) controls associated with remote access, customer logins, passwords, firm protocols to address customer login problems, network segmentation, and tiered access.

- Data Loss Prevention:
  1) robust controls in the areas of patch management and system configuration.
  2) monitor the volume of content transferred outside of the firm by its employees or through third parties, such as by email attachments or uploads.
  3) monitor for potentially unauthorized data transfers and how firms verify the authenticity of a customer request to transfer funds.

- Vendor Management:
  1) firm practices and controls related to vendor management, such as due diligence with regard to vendor selection, monitoring and oversight of vendors, and contract terms.
  2) how vendor relationships are considered as part of the firm's ongoing risk assessment process and how the firm determines the appropriate level of due diligence to conduct on a vendor.
- Training:
  1) how training is tailored to specific job functions and how training is designed to encourage responsible employee and vendor behavior.
  2) how procedures for responding to cyber incidents under an incident response plan are integrated into regular personnel and vendor training.
- Incident Response:
  1) acknowledge the increased risks related to cybersecurity attacks and potential future breaches.
  2) have established policies, assigned roles, assessed system vulnerabilities, and developed plans to address possible future events.

Again, the SEC attached a sample request for information and documents to be supplied to the examiners.

https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

May 17, 2017 – Cybersecurity: Ransomware Alert

This Risk Alert also provided some preliminary information on the current examination Initiative that the staff believed might be particularly relevant to smaller registrants:

- Cyber-risk Assessment: firms examined did not conduct periodic risk assessments of critical systems to identify cybersecurity threats, vulnerabilities, and the potential business consequences.
- Penetration Tests: Firms examined did not conduct penetration tests and vulnerability scans on systems that the firms considered to be critical.
- System Maintenance: Firms examined have a process in place for ensuring regular system maintenance however, some firms examined had a significant number of critical and high-risk security patches that were missing important updates.

https://www.sec.gov/files/risk-alert-cybersecurity-ransomware-alert.pdf

August 7, 2017 - Observations from Cybersecurity Examinations

Observations

"The staff noted an overall improvement in firms' awareness of cyber-related risks and the implementation of certain cybersecurity practices since the Cybersecurity 1 Initiative. Most notably, all broker-dealers, all funds, and nearly all advisers examined maintained cybersecurity related written policies and procedures addressing the protection of customer/shareholder records and information. This contrasts with the staff's observations in the Cybersecurity 1 Initiative, in which comparatively fewer broker-dealers and advisers had adopted this type of written policies and procedures."

- Most firms conducted periodic risk assessments of critical systems to identify cybersecurity threats, vulnerabilities, and the potential business consequences of a cyber-incident.
- Most broker-dealers and almost half of the advisers conducted penetration tests and vulnerability scans on critical systems.
- All firms utilized some form of system, utility, or tool to prevent, detect, and monitor data loss as it relates to personally identifiable information.
- Most firms had a process in place for ensuring regular system maintenance, including the installation of software patches to address security vulnerabilities.
- Information protection programs at the firms typically included relevant cyber-related topics, such as policies and procedures and response plans.
- Most firms maintained cybersecurity organizational charts and/or identified and described cybersecurity roles and responsibilities for the firms' workforce.
- Most firms had authority from customers/shareholders to transfer funds to third party accounts, but not all maintained policies and procedures related to verifying the authenticity of a customer/shareholder who was requesting to transfer funds.
- Most firms either conducted vendor risk assessments or required that vendors provide the firms with risk management and performance reports (i.e., internal and/or external audit reports) and security reviews or certification reports.

Issues Observed

While most firms maintained written policies and procedures addressing cyber-related protection of customer/shareholder records and information, a majority of the firms' information protection policies and procedures appeared to have issues, including:

- Policies and procedures were not reasonably tailored.
- Firms did not appear to adhere to or enforce policies and procedures, or the policies and procedures did not reflect the firms' actual practices.
- The staff also observed Regulation S-P-related issues among firms that did not appear to adequately conduct system maintenance, such as the installation of software patches to address security vulnerabilities.

Elements of Robust Policies and Procedures

- Maintenance of an inventory of data, information, and vendors.
- Detailed cybersecurity-related instructions, such as: penetration tests; security monitoring and system auditing; access rights; and reporting.
- Maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities, such as vulnerability scans of core IT infrastructure and patch management policies.
- Established and enforced controls to access data and systems.
- Mandatory employee information security training.
- Engaged senior management. The policies and procedures were vetted and approved by senior management.

https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf

My Perspective

The SEC calls these information sources Risk Alerts for a reason. The intent is to alert registrants to concerns that the SEC has about the way firms operate and issues with which the firms must deal. You can sign up for these alerts on the SEC's website. www.sec.gov/news/press/subscribe_updates.htm

In my view, if you are not watching for SEC alerts, somebody at the firm is not doing their job, and it might be you.

Please note, that every SEC Risk Alert includes the same last note:

"The adequacy of supervisory, compliance, and other risk management systems can be determined only with reference to the profile of each specific firm and other facts and circumstances."

Data Breach! What to Know About Where to Go...

By Louis Dempsey

Originally published May 2017

Regulators and law enforcement agencies aggressively pursue data breach cases focusing on the controls investment advisers and broker-dealers implement to prevent and detect a data breach. While significant emphasis is placed on the firm's preventative measures to detect and mitigate data breaches, there is little published to assist firms in the unfortunate instance where they may actually have been breached; this despite virtually every state having rules that require prompt reporting of such instances. In fact, how your firm deals with an attack may help mitigate the impact of regulatory action and criminal or customer litigation. Therefore, every firm should develop a robust response plan in the event of a breach that addresses the unique requirements of each jurisdiction in which it operates.

What is a Data Breach?

A data breach is an incident of unauthorized access to, or acquisition of, sensitive or confidential data. It may involve personally identifiable information ("PII") or personal health information. Although we most often think that a data breach involves only electronic data, we should also consider that PII is often contained in paper documents. Therefore, we must consider not only the protection of electronic PII, but also the destruction of documents that contain PII. Furthermore, breaches that occur at a third-party vendor, involving a firm's customer or proprietary data, may also be subject to state laws.

General State Requirements

In 2003, the state of California was the first state to enact a data breach notification law. Since that time, approximately 46 additional states have enacted laws addressing data breaches (Alabama, New Mexico and South Dakota are the exceptions). In general, state laws address the type of information that i covered, to whom notification of the breach must be reported, the timing of such notification, the assessment of potential harm, an civil liability in the event of a breach.

What information is covered?

While the definition of PII in many states is similar to the SEC's Regulation SP, the reporting obligations typically go beyond what is required under the federal rules. States generally define PII as:

1. The customer's first and last name in combination with some other data elements, such as a social security number, driver's license or state identification card, passport or similar information that may be used to verify identity; or
2. A financial account, debit or credit card number, along with a security or access code or password that would provide access to the customer's account.

Reporting Obligations

The reporting obligations under state laws are triggered by the acquisition, or reasonable belief of acquisition, of PII by an unauthorized person. Once triggered, firms must consider their reporting obligations to customers, government agencies, and others.

Reporting to Customers

For those states that have data breach laws, notification to customers is generally required. Firms are expected to investigate the breach immediately to determine the scope of the breach, and to take measures to restore the integrity of the system. If, during the investigation, the firm determines that there is no reasonable likelihood of harm, due to encryption or redaction of the data, then customer notification may not be required.

State data breach laws typically address the timing, content, and method of delivery of the notice to customers.

About the Author

Louis Dempsey is President at Renaissance Regulatory Services. He can be reached at louisdempsey@rrscompliance.com

1. *Timing*: In describing the timing of the notice, state laws use phrases such as "as expeditiously as possible", "without unreasonable delay", "immediately, but no later than 45 days from discovery of the breach", and "not later than 30 days after determination of the breach." Customer notification may be delayed upon request from a law enforcement agency if the agency believes notification would compromise or impede a criminal investigation.

2. *Content*: Notices to customers should include the name and contact information for the company, an explanation of what happened (including the date(s) of the breach), what information was involved, what the firm is doing to investigate and prevent a recurrence, and what the customer can do to protect his/her information going forward. Some states require that the notice include the toll-free numbers and addresses of the major consumer reporting agencies. Some states go further still, like California[1] and Connecticut,[2] and require the company to offer identity theft prevention and mitigation services if social security numbers are involved.

3. *Method of Delivery*: Generally, state laws permit reports to customers to be sent by written notice or by e-mail.

Reporting to Government Agencies

Not all state data breach laws require firms to notify the government of a breach, but, for those that do, the requirements vary widely. Some states have a threshold for the number of residents impacted (e.g., greater than 500) and identify the agency that must be notified. The state of New York, for example, requires that if any New York residents are impacted by a data breach, then the firm must notify the State Attorney General, the Department of State and the Division of State Police as to the timing, content and distribution of the notices, and the approximate number of affected persons.[3] The State of California requires that if more than 500 state residents are impacted as a result of a single breach, a firm must electronically submit a sample copy of the notice to the California Attorney General. Copies are maintained in a searchable database on the California Attorney General's website.

Reporting to Consumer Reporting Agencies

As with reporting to government agencies, state laws may also require data breaches to be reported to consumer reporting agencies. It is important to know what the state's requirement are for reporting to these agencies, and critically, the timing. Firms do not want their customers finding out about a breach from some other entity.

Reporting to Third-Parties

If a firm or its vendors maintain documents or data for third parties, and that data contains PII, the holding firm must notify the third-party owner of the information immediately upon discovery of the breach. This would include PII maintained on behalf of affiliates, custodians, and advisers where a subadvisory arrangement exists. For example, if a custodian brokerdealer maintains PII on the clients of its affiliated investment adviser, then the broker-dealer would notify the adviser of a breach. Similarly, if a sub-advisor is breached it would be required to notify the adviser who has the primary relationship with the customer. These obligations should be documented in contractual agreements between the entities and in each entity's compliance program.

Companies should be aware that the laws to which they are subject are based on the location of the affected customers. Thus, in the event of a breach, the company may find itself being accountable to several states on a single breach.

Penalties for Non-Compliance with State Data Breach Laws

Companies should be aware that the laws to which they are subject are based on the location of the affected customers. Thus, in the event of a breach, the company may find itself being accountable to several states on a single breach. For this reason, your firm must assess the reporting requirements for each state in which it operates or has customers.

Many state laws provide for civil penalties in the event of violations of their data breach laws. The penalties may be based on several criteria, e.g., the number of residents in the state who were not notified of the breach or the number of days the notification was delayed. Additionally, in some states, the Attorneys General could bring an action to recover economic damages resulting from a violation.

Finally, some states require the firm providing the notice to offer identity theft prevention and mitigation services to the customers at no cost for at least one year.

Safe Harbor for Use of Encryption

Although there are significant potential costs for a breach, some state data breach laws provide an exemption for firms that use encryption. If the information is encrypted, redacted or truncated (e.g., last four digits of the social security number or credit/debit card), and the encryption key was not accessed or acquired by the hackers, the reporting requirements in the statutes would not apply. Of course, firms must ensure that the encryption methods are industry standard and that the hackers did not acquire the encryption keys through other means.

Resources

Knowing where to start is critical. The varying state requirements create a multitude of reporting obligations that firms must be aware of to avoid significant regulatory actions or litigation that could cripple a firm. Researching all of the state requirements can be onerous, but there are resources. We've listed below some resources that can help you to begin developing your data breach incident response plan.

The National Society of Compliance Professionals

National Conference of State Legislatures Website (as of 2/24/2017):

California Attorney General searchable database

Privacy Rights Clearinghouse Data Breaches

Data Disposal Laws

Knowing where to start is critical.

Conclusion

As government agencies and the public focus more aggressively on data breaches, it is important for investment advisers and broker-dealers to ensure that they assess the requirements for data breach disclosure in each jurisdiction in which they operate. It may not matter who your primary regulator is, as data breach laws are unique to each jurisdiction. Determining what the requirements are for each jurisdiction in which you operate is critical to developing your response plan and may reduce your risk exposure to regulatory, civil or criminal actions.

(Endnotes)

1. California Civil Code 1798.82(d)(2)(G), effective 1/1/2015
2. Connecticut General Statutes Sec.6. Section 36a-701b.(b)(2)(b), effective 10/1/2015
3. NY Gen. Bus. Law 899-aa.8.(a)

SEC and States are Upping Their Cyber Game, Are Your Doing the Same?

By Brian Rubin, Michael Bahar, Amber Unwala, Trevor Satnick

Originally published November 2017

September 2017 saw no respite from the relentless pace of cyber developments, not only from the perspective of rapidly evolving attacks, but also from the perspective of dynamic federal and state regulatory moves. In particular, on September 25, 2017, the Securities and Exchange Commission (SEC) announced a new enforcement initiative to address growing cyber-based threats and protect retail investors.[1] The initiative established a Cyber Unit to target misconduct, a move that could place further pressure on broker-dealers and investment advisers already feeling the heat from an uptick in cyber-related exams and the relentless onslaught of cyber intrusion attempts. Second, a day earlier, the North American Securities Administrators Association (NASAA) announced that state securities examiners conducted over 1,200 coordinated examinations of state-registered investment advisers between January and June 2017, finding 698 cybersecurity-related deficiencies.[2]

Given the advancing threats and the increasing regulatory scrutiny, broker-dealers and investment advisers should consider acting with increased urgency to further prepare themselves, focusing in particular on having written cyber policies that are regularly updated to account for the latest threats. The severity and frequency of attacks are only growing, while the tolerance among regulators for failing to take sufficient preventive steps is only diminishing. Against both attackers and regulators, the best offense truly is a good defense, and regulators are strongly indicating that it is not enough to simply have a defense; but rather, that defense must also evolve to keep pace with the rapidly evolving offense.

The SEC: What the Cyber Unit Will Do

With the creation of the Cyber Unit, the SEC is beefing up its technical expertise and demonstrating that it too will evolve and adapt as cybersecurity threats become more advanced. The agency is making it increasingly clear that it expects those it regulates to up their games as well.

The unit will function as part of the SEC's Enforcement Division to target misconduct along six cyber-related priority areas:

- Market manipulation schemes involving false information spread through electronic and social media;
- Hacking to obtain material nonpublic information;
- Violations involving distributed ledger technology and initial coin offerings;
- Misconduct perpetrated using the dark web;
- Intrusions into retail brokerage accounts; and
- Cyber-related threats to trading platforms and other critical market infrastructure.

By examining each of these areas in depth, this article tries to discern the SEC's key concerns and suggests issues that firms may want to consider addressing, before facing the SEC in an examination or in an enforcement action.

Market Manipulation Schemes

With the spread and growing influence of "fake news" to manipulate political outcomes (and with further proof of intentional nation-state involvement in spreading such false stories),[3] it is no surprise that the SEC is concerned

About the Authors

Brian Rubin is Partner at Eversheds Sutherland. He can be reached at brianrubin@eversheds-sutherland.com.
Michael Bahar is Partner at Eversheds Sutherland. He can be reached at michaelbahar@eversheds-sutherland.com.
Amber Unwala is an Associate at Eversheds Sutherland. She can be reached at amberunwala@eversheds-sutherland.com.
Trevor Satnick is a Staff Attorney at Eversheds Sutherland. He can be reached at trevorsatnick@eversheds-sutherland.com.

1. SEC Press Release, "SEC announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors" (Sept. 25, 2017), https://www.sec.gov/news/press-release/2017-176.
2. "State Investment Adviser Examinations Uncover Cybersecurity Deficiencies" (Sept. 24, 2017) http://www.nasaa.org/43287/state-investment-adviser-examinations-uncover-cybersecurity-deficiencies/.
3. Scott Shane and Mike Isaac, Facebook to Turn Over Russian-Linked Ads to Congress, NY TIMES (Sept. 21, 2017), https://www.nytimes.com/2017/09/21/technology/facebook-russian-ads.html.

about the use of targeted misinformation via social media to manipulate market outcomes.

The SEC will likely be on the lookout for companies hoping to turn an illicit profit by creating or spreading known misinformation via the internet. The SEC could bring fraud cases against those who disseminate false information to manipulate the market, and aiding and abetting cases against those who negligently spread the false information. In fact, the SEC has already started. In 2015, the SEC filed securities fraud charges against a Scottish trader whose false tweets caused sharp drops in the stock prices of two companies and triggered a trading halt in one of them.[4]

In light of the growing prevalence of intentionally fake stories, it may be prudent for firms to have proactive policies in place that not only explicitly prohibit the dissemination of knowingly false information, but that also require some form of verification before sharing certain market-related news with clients and prospective clients.

Hacking to Obtain Material Nonpublic Information

The SEC's new enforcement unit will be on the lookout for hackers that infiltrate broker-dealers and investment advisors to trade on nonpublic information or try to manipulate the

to investigate the breach immediately to determine the scope of the breach, and to take measures to restore the integrity of the system. If, during the investigation, the firm determines that there is no reasonable likelihood of harm, due to encryption or redaction of the data, then customer notification may not be required. State data breach laws typically address the timing, content, and method of delivery of the notice to customers.

market, something from which even the SEC is not immune.[5] While firms are victims of a cyberattack, the SEC may nonetheless bring "strict liability" enforcement actions against them if they had deficient proactive policies or procedures in place. While not a market manipulation case per se, in September 2015 the SEC brought an enforcement action against an investment adviser that had been breached, compromising the personally identifiable information (PII) of approximately 100,000 individuals, including thousands of the firm's clients (although there was no evidence that any of the information was used).[6] The SEC alleged that the firm violated the "Safeguards Rule" over a four-year span by failing to adopt written policies and procedures to ensure security of 100,000 individuals' personally identifiable information. The "Safeguards Rule" in Rule 30(a) of Regulation S-P requires certain policies and procedures for financial institutions to put into place to ensure confidentiality of their client's information.[7] Similarly, in April 2016, the SEC brought an action against a dually registered broker-dealer/investment adviser that had an employee impermissibly access and transfer data regarding approximately 730,000 accounts to his personal server, which was ultimately hacked by third parties.[8] The SEC alleged that the firm failed to adopt written policies and procedures reasonably designed to ensure the security of customer records and information.

Accordingly, to try to avoid future enforcement actions, broker-dealers and investment advisors may want to focus on establishing and implementing written, proactive cybersecurity policies that are regularly updated to account for the latest hacker tactics and techniques. Cyber is a dynamic, if not volatile, environment—the best laid plans of last year may not mean much this year.

Violations Involving Distributed Ledger Technology and Initial Coin Offerings

The SEC is signaling that it will not allow distributed ledger technology (DLT) or cryptocurrency to be used in a way that evades regulations, results in market manipulation, or is used to perpetrate frauds on investors. Unlike China, which has outright banned cryptocurrency—a move that has further a black market of cryptocurrency trading[9]—the SEC is indicating more of a desire to focus on regulating it.

On September 29, for example, the SEC brought its first enforcement action involving two Initial Coin Offerings (ICOs) for "defrauding investors" by selling these "unregistered securities" purportedly backed by investments in real estate and diamonds[10].

4. SEC Press Release, "SEC Charges: False Tweets Sent Two Stocks Reeling in Market Manipulation" (Nov. 5, 2015), https://www.sec.gov/news/pressrelease/2015-254.html.
5. Just a week before the announcement of the creation of the Cyber Unit, the SEC reported that its own EDGAR system fell victim to a cyberattack, possibly allowing the bad actors to trade on insider information. SEC Press Release, "SEC Chairman Clayton Issues Statement on Cybersecurity" (Sept. 20, 2017), https://www.sec.gov/news/press-release/2017-170.
6. SEC Press Release, "SEC Charges Investment Adviser With Failing to Adopt Proper Cybersecurity Policies and Procedures Prior To Breach" (Sept. 22, 2015), https://www.sec.gov/news/pressrelease/2015-202.html.
7. 17 C.F.R. § 248.30.
8. SEC Press Release, Firm "Failed to Safeguard Customer Data," (June 8, 2016), https://www.sec.gov/news/pressrelease/2016-112.html.
9. Chuin-Wei Yap, After Bitcoin Crackdown, Cryptocurrencies Go Clandestine in China, WSJ (Oct. 4, 2017), https://www.wsj.com/articles/in-china-cryptocurrency-sales-persist-in-the-shadows-1507109400.
10. SEC Press Release, "SEC Exposes Two Initial Coin Offerings Purportedly Backed by Real Estate and Diamonds" (Sept. 29, 2017), https://www.sec.gov/news/press-release/2017-185-0.

At this juncture, however, it remains unclear whether the SEC will mandate that all or some ICOs be registered as securities.

Misconduct Perpetrated Using the Dark Web

As part of its effort to keep up with the rapidly evolving techniques to engage in insider training and market manipulation, the SEC is now putting potential bad actors on notice that it will be shining the light on the so-called dark web, where bad actors have traditionally gone to anonymously buy and sell improperly obtained information and tools to conduct nefarious cyber activity. Therefore, if firms are not periodically—either themselves or through third parties—monitoring the dark web for stolen firm information that could impact their business or clients, it is possible that the SEC may focus on that failure.

Intrusions Into Retail Brokerage Accounts

The SEC is also calling out the practice of hacking retail brokerage accounts to manipulate markets. By making certain trades, the hacker can try to inflate the prices of holdings that he or she possesses or decrease prices to facilitate successful short selling. In 2016, the SEC charged a man from the UK with breaking into numerous accounts and placing unauthorized trades, ultimately leading to profits within minutes of trading the same stocks within his own account.[11] While the broker-dealer was not charged in that case, it is possible that in future cases, the SEC could charge the firm for allowing the hack to take place.

Therefore, if firms are not periodically—either themselves or through third parties—monitoring the dark web for stolen firm information that could impact their business or clients, it is possible that the SEC may focus on that failure.

In another case, a dually registered broker-dealer/investment adviser had experienced a series of computer system security breaches in which an unauthorized person or persons had accessed and traded, or attempted to trade, customer accounts. The SEC alleged that the firm had failed to implement increased security measures and adopt policies and procedures reasonably designed to safeguard customer information as required by Regulation S-P. Thus, broker-dealers and investment advisers may want to consider assessing what the scope of their data is and adopt procedures to attempt to prevent intrusions, and to respond to an intrusion if one takes place.

Cyber-Related Threats to Trading Platforms and Critical Market Infrastructure

The SEC is warning that hackers exploit blind-spots and nodes where they can have out-sized effects, so that those entities, such as trading platforms that may think they have low risk of attack, may consider taking more appropriate precautions. For example, instead of bringing down one website, hackers in 2016 launched a DDOS attack via simple devices like connected coffee pots to attack the internet itself. The hack took control of Internet of Things (IoT) devices with lax security protocols and used these devices to overload an internet infrastructure company's servers with bogus internet traffic. The attack successfully brought the company to its knees and took down several websites belonging to some of the internet's largest household names for the better part of a day.

Instead of bringing down one website, hackers in 2016 launched a DDOS attack via simple devices like connected coffee pots to attack the internet itself.

Accordingly, the SEC is sounding the alarm that trading platforms and stock exchanges are vulnerable to attacks of this nature and should, therefore, consider taking proactive, risk-based steps to prevent system-side failures due to cyberattacks. The SEC could possibly bring cases against firms with trading platforms, or even stock exchanges, if they have inadequate cybersecurity system, policies and procedures.

The States

Like the SEC, the states are also focused on what proactive steps should be taken—and they are finding that a number of state-registered investment advisers have not taken those steps. On September 24, 2017, NASAA issued a report based on over 1,200 examinations of such firms. NASAA noted that state securities regulators found 698

11. SEC Press Release, Firm "Failed to Safeguard Customer Data," (June 8, 2016), https://www.sec.gov/news/pressrelease/2016-112.html.

deficiencies that involved cybersecurity. The top five deficiencies were: inadequate or no cybersecurity insurance; no testing of cybersecurity vulnerabilities; a lack of procedures regarding securing and/or limiting access to devices; no technology specialist or consultant on staff; and a lack of policies and procedures regarding hardware and software updates or upgrades.

NASAA used the data to generate a list of cybersecurity best practices for investment advisers. NASAA encouraged investment advisers to: prepare and maintain records by backing them up; maintain client information; revise Form ADV and disclosure brochures; implement safeguards through cybersecurity policies and measures; and prepare a written compliance and supervisory procedures manual.

NASAA found policies and procedures to be adequate when they, for example, require and enforce frequent password changes, locking of devices, reporting lost devices, and creating specific roles and responsibilities for people to assess these requirements on a frequent basis. To minimize threats posed by data breaches, firms may want to consider routinely backing up devices and storing the underlying data in a separate, remote location. Firms may also want to consider regularly testing backup procedures to ensure their suitability. Similarly, firms may want to consider whether email communications should be sent securely, especially where they involve identifiable information regarding a client. Firms also may want to review training of their employees and registered persons to try to ensure that each person understands her role and responsibility.

As the virulence and prevalence of cyberattacks increase, regulators at both the federal and state levels are looking to enforce sound cyber hygiene on the front end, and they are increasingly requiring that proactive plans and policies be updated regularly to account for the rapidly evolving threats. The SEC's creation of the Cyber Unit coupled with an uptick in exams and the relentless onslaught of cyber intrusion attempts should put broker-dealers and investment advisers on notice that what they do and do not do before any breach is what matters most. Accordingly, firms and funds should remain proactive and place continued emphasis on maintaining—and regularly updating—their cybersecurity readiness. Attackers are evolving, and so too must the defenders.

Office of Compliance Inspections and Examinations Identifies Common Weaknesses in Cybersecurity Compliance

By Scott Sherman and Josh Lewin

Originally published November 2017

While state governments have always possessed the authority to impose and enforce cybersecurity regulations, traditionally, they have allowed federal agencies like the FTC or the SEC to spearhead the enforcement efforts. In light of recent high-profile data breaches, this trend has shifted course, throwing financial firms into the enforcement crosswinds of both the federal regulatory agencies and the state governments. To this end, the Massachusetts Attorney General filed a complaint against Equifax on September 17, 2017, alleging violations of the Massachusetts Data Security Regulations. While it remains to be seen where the bulk of enforcement will come from, it is clear that cybersecurity is a priority for both state legislatures and regulatory agencies. As regulation and enforcement continue to progress, broker-dealers, investment advisers, and investment companies must remain alert to their compliance obligations.

The Office of Compliance Inspections and Examinations Report

On August 7, 2017 the Office of Compliance Inspections and Examinations ("OCIE"), in accordance with its Cybersecurity 2 Initiative, published a report detailing its examination of cybersecurity compliance amongst financial firms. The OCIE's National Examination Program staff examined a group of 75 broker-dealers, investment advisers, and investment companies registered with the SEC. The examination tested the firms' procedures and controls surrounding cybersecurity preparedness. The OCIE Report is indicative of the issues that most commonly plague financial services industry firms. This article aims to provide practical guidance on how to resolve these issues.

Does the OCIE Report set a standard/why does it matter?

While many industry professionals seek clear standards for cybersecurity compliance, bright-line rules remain elusive. Unfortunately, compliance with the findings and measures suggested by the OCIE Report do not create an industry standard nor a safe harbor. However, the OCIE Report is perhaps the most informative resource on real-world weaknesses in compliance and practical guidance solutions.

What are the areas of weakness that the OCIE identified?

Policies and procedures were not reasonably tailored because "they provided employees with only general guidance, identified limited examples of safeguards for employees to consider, were very narrowly scoped, or were vague, as they did not articulate procedures for implementing the policies.

Almost all firms investigated maintained some form of written policies and procedures pertaining to the cyber-protection of client records, however, the report concluded that a majority of the firms' information protection policies were deficient. Common problems include:

The policies and procedures "were not reasonably tailored" to protect client information in accordance with Regulation S-P, which requires firms to customize security policies in order to protect client information. The policies and procedures were not reasonably tailored because "they provided employees with only general guidance, identified limited examples of safeguards for employees to consider, were very narrowly scoped, or were vague, as they did not articulate procedures for implementing the policies."

About the Authors
Scott Sherman is Partner at Nelson Mullins. He can be reached at scott.sherman@nelsonmullins.com.
Josh Lewin is an Associate at Nelson Mullins. He can be reached at josh.lewin@nelsonmullins.com.

In some instances, where the policies and procedures were proper, the firms did not "adhere to or enforce policies and procedures, or the policies and procedures did not reflect the firms' actual practice." For example, where some firm policies and procedures required annual penetration tests, ongoing reviews of supplemental security protocols, or continued employee cybersecurity training, the firm simply failed to enforce their own policies and procedures.

The OCIE Report also found areas of concern with Regulation S-P among firms that did not adequately conduct system maintenance. Some firms used outdated operating systems that were no longer supported by security patches.

Finally, some firms were cited for their lack of remediation efforts. The report notes that "high-risk findings from penetration tests or vulnerability scans did not appear to be fully remediated in a timely manner."

Practical Guidance for Compliance

To comply with cybersecurity regulations it is indispensable to maintain and adhere to vigorous written policies and procedures. The OCIE Report concluded that the following suggestions were common amongst the "robust policies and procedures" that it reviewed.

1. Memorialize the policies and procedures in a formal writing.
2. Provide situational instruction and training to employees.
3. Include step-by-step guides and instructions, rather than large lists of rules and requirements.
4. Conduct penetration tests and provide specific information and instructions to review the effectiveness of security solutions.
5. Monitor access rights by recording all requests for access. Have a policy in place that specifically addresses modification of access rights in scenarios like employee hiring, changing positions or responsibilities, and terminating employment.
6. Maintain an inventory of data, information, and vendors. Policies and procedures should include an inventory of data and information, along with classifications of the risks, vulnerabilities, data, business consequences, and information regarding each service provider and vendor.
7. Limit access to controls and access to data and systems. Strong firm policies may include:
    a. Restrictions on access to outside networks when using firm equipment
    b. Restrictions on use of mobile devices that connect to the firm's systems, such as requiring passwords or encryption software
    c. Requiring third-party vendors to provide records of their activity on the firm's networks
    d. Requiring immediate termination of access to terminated employees
8. Make employee training mandatory at on-boarding and periodically thereafter. Institute a policy to ensure this training is complete.
9. Senior management should be aware of and approve cybersecurity policies.
10. Enact a provision to ensure that all policies and procedures are actually adhered to and executed as planned. This might involve hiring a Chief Compliance Officer or formally assigning this responsibility to an already existing position.

Where will the SEC focus compliance enforcement?

The SEC's 2017 Examination Priorities Letter fortified the SEC's rigorous stance on cybersecurity, once again focusing on protection of client information. The Examination Letter, as well as the OCIE Report, indicate that the SEC is focused on compliance procedures and controls, as well as implementation of those procedures and controls.

In a large enforcement action against Morgan Stanley last year, the SEC issued an order finding that Morgan Stanley "failed to adopt written policies and procedures reasonably designed to protect customer information." Morgan Stanley settled the charges by agreeing to pay a $1 million penalty. The SEC will likely continue to enforce cybersecurity regulations with a particular focus on adherence to the policies and procedures detailed in the OCIE Report.

The key distinction between state law and regulatory enforcement is the type of event that must take place in order to trigger liability or disciplinary measures.

Consequences of Non-Compliance

The consequences of non-compliance will vary based on whether an action is pursued under state law or by a regulatory agency. A claim under state law will subject the firm to civil liability, whereas a regulatory enforcement action will subject the firm to administrative discipline.

The key distinction between state law and regulatory enforcement is the type of event that must take place in order to trigger liability or disciplinary measures. Federal regulatory agencies, like the SEC, may discipline a firm for simply failing to maintain adequate policies and procedures to safeguard consumer information (no data breach is necessary!). Whereas, under state laws, liability will be triggered only after an actual breach of cybersecurity.

In the event of a cybersecurity breach, firms must be aware of their obligation to report the breach to the appropriate individuals or entities.[1] State laws vary as to who firms must notify and when firms must notify them.[2] To complicate matters even further, state laws vary as to what level of harm the data breach must cause in order to trigger a notification requirement. In some states, like California, every data breach must be reported. In others, like South Carolina, a data breach does not need to be reported if the firm reasonably believes that illegal use of data has and is not reasonably likely to occur and use of information does not create a material risk of harm to a resident.

Thus, in the event of a data breach it is important for broker-dealers, investment advisors, and investment companies to be aware of their state-imposed disclosure obligations, as they may vary.

Civil penalties under state laws may require firms to pay economic damages and to offer identity theft prevention services for free. Regulatory enforcement actions may result in censures and financial penalties.

Conclusion

While broker-dealers, investment advisers, and investment companies are subject to state cybersecurity regulations and enforcement, the lion-share of these proceedings have been brought by the federal regulatory agencies. With more states enacting cybersecurity legislation, financial firms should keep a keen eye on enforcement patterns. As always, now is the appropriate time to incorporate some of the guidance provided here and ensure that your firm is in compliance with its cybersecurity obligations.

Cyber Security is so big right now that SEC Commissioner is floating an idea to delay reporting of certain data that it requested because it isn't sure if it can protext it

SEC Involvement in Cyber Security

SEC Involvement in Cyber Security

SEC Spotlight on CyberSecurity Regs

Testing and Compliance Reports

Firms Worst Mistakes
Best Practices in FINRA Report:

1. To read more about reporting obligations see Louis Dempsey's Article "Data Breach! What to Know About Where to Go.." in the May 2017 NSCP Currents
2. To date, there is no federal law on data breach notification requirements; however, Rhode Island Congressman Jim Langevin reintroduced the Personal Data Notification and Protection act in September 2017 in an attempt to provide a uniform standard.

Compliance Protocols for Dealing with Current Cybercrimes

By Craig Watanabe

Originally published June 2017

This article discusses some recent phishing expeditions, and provides steps firms can take to help protect themselves against these threats. In an effort to provide practical and actionable guidance, this article references certain products and vendors; however, these are provided as suggestions only and should not be considered specific recommendations by the author or NSCP.

According to a Data Breach Investigations Report published by Verizon in 2016, investors.[1] there has been a definite upward trend in the number of people clicking on "phishing" emails since 2014. Phishing is a type of social engineering used by hackers to trick people into introducing a virus into their computer or revealing confidential information.

Approximately 70% of cyber-breaches entail a compromised user.

Examples of Phishing Attacks

Approximately 70% of cyber-breaches entail a compromised user. Unfortunately, hackers are getting very sophisticated. Below are three examples of current phishing scams that have trapped a high percentage of victims.

Example #1 – Phishing

An employee receives the following email, which appears to have come from an HR officer:

> *"It has been brought to our attention there was a problem with ADP that may have affected your 2016 W-2 form. Please read the attached memo and notify me if you have been impacted."*

The employee clicks on the attachment, which reads:

> *"Please check your December 29, 2016 pay stub and reconcile the figures with your 2016 Form W-2. If the numbers match, you do not need to take any further action. However, if there are any discrepancies please notify HR and we will issue a corrected 2016 Form W-2."*

Of course, the pay stub and W-2 match, but the attachment contained a virus so the employee's computer and possibly the firm's network has been infected.

Example #2 – Whaling

All employees (except the CEO) receive the following email, which appears to have come from the firm's CEO:

> *"One of our largest clients is opening a Pizza Hut within walking distance of our office at 123 S. California Blvd. The owner wants to give each employee a free medium pizza! Please click on the button below to download your coupon for the free pizza, and please spread the word to support our valued client."*

The email has all of the Pizza Hut branding and that free pizza button looks inviting, but clicking on the button reveals an error message that reads "HTTP 404 – File Not Found," and a virus is deposited into the computer.

Example #3 – Spear Phishing

A firm has posted job descriptions on several bulletin boards stating interested parties should send a resume to humanresources@abc-company.com. A hacker trolls for companies that have posted job descriptions and attempts

About the Author

Craig Watanabe is a Senior Compliance Consultant with Core Compliance & Legal Services, Inc. He can be reached at craig.watanabe@corecls.com

1. See http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

to "spear phish" the HR person by sending an email with a fake resume attached. Everything looks normal, and since the HR person is expecting to receive resumes, nothing appears suspicious. However, the resume has a virus attached that activates when the resume is opened.

Compliance Protocols Geared for Prevention

User Awareness Training

Knowledge is power, so it's important to continually train employees on current types of threats and what can be done to prevent cyberattacks. Below are some tips for identifying phishing emails:

1. Check the URL address to help determine legitimacy
2. Confirm the domain name in the sender email address appears correct
3. Check the content of the email (if viewable without opening)
    a. Does it appear to be something that would normally sent from the sender?
    b. Does it contain any misspelled words?
    c. Is it asking for confidential information?
    d. Does it require opening a link or attachment?
4. Don't click on links or attachments if emails contain threats
5. Be alert and never trust without obtaining verification

Implement Phishing Simulations

Simulated phishing emails, which track who opens the email and who clicks on the associated link or attachment, can be sent periodically to employees. For this type of training to be effective, employees should not be informed of the simulated emails, and those who open the emails should receive a short, mandatory training session.

Simulated phishing emails, which track who opens the email and who clicks on the associated link or attachment, can be sent periodically to employees.

Phishing simulations and the subsequent training help to reduce the "click" rate. In addition, this improvement is measurable and documented.

Suggested Vendors: InfoSec Institute (www.infosecinstitute.com) and KnowBe4 (www.knowbe4.com) offer various user awareness training tools and educational services.

Two-Factor Authentication ("2FA")

Cybersecurity is a regime to prevent unauthorized access. The primary mode of authentication is a username and password, and misappropriating these credentials is one of the most common ways to breach a network.

2FA is an internal control that greatly enhances security by requiring a second form of identification in addition to the username and password. Examples of 2FA are answering challenge questions, recognizing chosen images on a website, SMS text message tokens (a six-digit one-time code that must be entered), and fobs that generate security codes.

2FA is becoming standard. In 2016, in the wake of the highly publicized breach of a government employee database, President Obama mandated 2FA for all government agencies. In addition, banks are required to use 2FA, and a number of popular websites and services have chosen to offer 2FA, including Microsoft Office 365, Amazon, Facebook, and Gmail. The capability is there. Users simply need to enable the additional security. 2FA is economical and can be very effective in preventing unauthorized access.

Suggested Vendors: RSA (www.rsa.com) and Yubico (www.yubico.com) offer a variety of 2FA products and services.

Endpoint Monitoring and Protection

Each electronic device that connects to a firm's network is an "endpoint," which needs to be protected. The endpoint device could be a mobile device, laptop computer, home computer, and/or workstation in the office. Endpoint monitoring allows a firm to oversee network access activity in real time and, in some cases, prevent attempted cyberattacks.Suggested Vendors: Entreda (www.entreda.com) and Symantec (www.symantec.com) offer endpoint monitoring products.

Conclusion

Maintaining a strong cybersecurity program is a daunting task for firms given the barrage of cyberattacks that continue to undermine reasonable efforts. Compliance personnel need to work closely with IT personnel to help ensure adequate protections are in place. Risk assessments should be performed annually and ongoing employee training is a must. It's also very important that senior management ensures adequate resources continue to be allocated to the firm's cybersecurity program.

NSCP
NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

MEMBERSHIP

"NSCP Membership promotes professional growth, development and unification of compliance professionals within the financial services industry. NSCP members have full access to a community of like-minded people, exceptional experiences, practical and compelling content, and essential tools that empower and inspire."

– NSCP Executive Director, Lisa Crossley on the Benefits of Membership

Community

Join our Online and Industry Forums and benefit from the collective expertise of the NSCP Member Community.

Learning

Industry leading events, deliver the timeliest information our members need to stay ahead of the curve. Receive preferred member pricing for NSCP's exclusive on-site events.

Regulatory Engagement

NSCP MemberVoice

NSCP is the only nonprofit representative organization for the compliance profession, uniquely positioned to take an independent stance with respect to industry developments, and to promote unbiased consensus with respect to initiatives from the SEC, the SROs, and Capitol Hill.

Knowledge

Best in class resources, designed and delivered by professionals that understand your needs:
NSCP Currents • NSCP Resource Library • Introductions to local Roundtables • Access to the NSCP Jobline for Resumes & Job postings

MEMBERSHIP BENEFITS