New Cybersecurity Regulations Demystified: A Brief to Fund Managers on How to Get Started

By Oleg Bogomolniy, Chief Security Officer, InfoHedge Technologies, LLC

In an industry accustomed to changing regulations, fund managers now have two more to deal with – but this time, they are not financial in nature. New cybersecurity regulations have been released by the U.S. Security and Exchange Commission (SEC) and National Futures Association (NFA) aimed at bringing the alternative investment industry on par with current cybersecurity threats. These regulations go well beyond the standard firewall, expecting fund managers to become the governing power of cybersecurity in their firms. To be in full compliance is indeed much like eating an elephant. How does one eat an elephant? One bite at a time, of course. In this brief, we will demystify the new cybersecurity regulations one digital byte at a time, and help you to translate them into a meaningful strategy.

INTRODUCTION

Over the past three decades, the alternative investment industry has grown to become one of the most valuable contributors to the global economy, managing trillions of dollars. This industry is no stranger to oversight, as it's controlled by some of the toughest, business-impacting regulations the global financial system has ever seen: Dodd-Frank, AIFMD, GLBA, SOX, FISMA, among other regulations planned for 2016 and beyond. However, the recent cybersecurity initiatives from the SEC and NFA caught many fund managers by surprise for two main reasons. First, most of the firms impacted by these regulations either do not have their own IT departments, or only rely on rudimentary IT support personnel. Second, unlike funds' bigger cousins, banks, the alternative investment industry has been laying low under cyber-threat radars. There just hasn't been much value in hacking into a hedge fund. So why now? To understand the thinking and methodology of the regulators behind these cybersecurity initiatives, we first need to understand the ingredients in the mix.

THE RECIPE FOR DISASTER

Fast and furious

Even though cybersecurity has not been on the top priority list for the alternative investment industry in the past decade, technology, on the other hand, has unequivocally been one of its biggest enablers. This is in reference to quantitative analysis, High Frequency Trading (HFT), and other algo-trading strategies, or "the secret sauce": VWAP, TWAP, high-tech front-running, delta-neutral trading, rebalancing index fund, arbitrage opportunities, or just simply following trends. Algo-trading redefined the need for speed of trading computer connections and made every microsecond count. However, despite lucrative profits, algo-trading proved to be naturally capable of detrimental powers, as seen in the 2010 and 2015 Flash Crashes. So why can't the same powers be harnessed for deliberate manipulations? What would stop an adversary to create malicious algorithms to paralyze financial exchanges? Rather than simply plugging in algorithms into financial markets from anywhere, one could covertly "tap" into legitimate trading models used by a firm with weak cyber-defenses. Now the perpetrator can take any "cyber-position":

- Financial gains from hidden trades
- Offering "for hire" services to artificially manipulate the market conditions
- Stealing proprietary trading strategies, or
- Simply selling a segue into a firm with access to financial exchanges to a higher bidder

You have to pick up every stitch, must be the season of the breach

In 2015, there were over 700 major security breaches with price tags averaging over (US) $1.57M[1]. This number is expected to grow in 2016, with more industry sectors being mandated to report security breaches. The financial industry was the target of over 80% of these attacks and breaches in 2015. The top three categories of security incidents in the alternative investment industry are:

- Cyber-crime
- Cyber-espionage
- Insider misuse (deliberate or incidental)

Cyber: the new commodity

Cyber is now one of the most valuable commodities. Cybercrime has grown into its own $400+ billion industry[2] and has plenty of room for growth potential. Underground markets are booming with counterfeit credentials, premium credit cards, online bank accounts, malware for sale, hacking services-for-hire, hacker tutorials, and much more. The competition among cybercriminals themselves is getting increasingly intense, which drives down the price for stolen cyber. So now they tend to target wealthier victims – a serious concern for the alternative investment industry.

What's your firm's credit is worth?

In 2015, Moody's Corp. announced their plans to include cyber-defense capabilities in its analysis of the creditworthiness across all sectors. Data breach detection and incident response will be a part of their analysis. Following Moody's announcement, Standard & Poor's revealed they had begun querying financial institutions using a list of 16 questions to gauge their cybersecurity readiness. Those questions include:

- How long has it typically taken to detect a cyberattack?
- What containment procedures are in place if a business is breached?
- How many times was the business the target of a high-level attack during the past year, and how far did it reach in the system?
- What's the internal phishing success rate?
- What kind of expertise about cyberattacks exists on the board of directors?
- How much does the business spend on cybersecurity, what resources does it devote, and what is the total tech budget this year versus last?

It's not what your country can do for you…

The rise in adversarial sophistication and continuous persistence of advanced threats against American entities prompted Executive Order 13694, signed by the President Barack Obama in April of 2015 and authorizing action against "malicious cyber actors whose activities are directed against U.S. critical infrastructure, our companies, or our citizens and could threaten the national security, foreign policy, economic health, or financial stability of the United States."

To summarize, the key risks for the alternative investment industry that dictated the need for new cybersecurity regulations are:

- Covert manipulation of various types of trading (e.g., algorithmic) for financial gains or malicious intent (crashing the market)
- Cyber-espionage: theft of intellectual property (IP), confidential or investors' personal information
- Cyber-extortions: "siege" of computer systems for monetary compensation
- Malware: inability to conduct business for prolonged period of time

---

[1] Ponemon Institute Research Report. (2015, May). 2015 Cost of Data Breach Study: Global Analysis. Retrieved from IBM Security: http://www-03.ibm.com/security/data-breach/

[2] Center for Strategic Internet Studies. (2014). Net Losses: Estimating the Global Cost of Cybercrime. Retrieved from The Center for Strategic and International Studies: http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

CYBERSECURITY INITIATIVES

How it's made

In 2014, the SEC was tasked to provide guidelines for creating and enhancing cybersecurity programs to its registered entities. The SEC took pragmatic, phased approach to build its own pyramid, using cybersecurity best practices:

- NIST Cybersecurity Framework
- CIS Controls for Effective Cyber Defense (formerly Top 20 Critical Controls)

A year later, the SEC published the results of their ongoing Cybersecurity Examination Initiative conducted by the Office of Compliance Inspections and Examinations (OCIE), including specific six areas of focus for succeeding rounds of audits:

1. Cybersecurity Governance and Risk Assessments
2. Access Rights and Controls
3. Data Loss Prevention (DLP)
4. Vendor Management
5. Cybersecurity Incident Response
6. Cybersecurity Awareness & Training

As of March 2016, NFA's Cybersecurity Interpretive Notice went into effect. Approved by the Commodity Futures Trading Commission (CFTC), it requires "Member firms to adopt and enforce written policies and procedures to secure customer data and access to their electronic systems." NFA has adopted the SEC's approach of addressing cybersecurity threats, focusing on the six main areas mentioned earlier.

Now let's take a closer look into each area and define "quick wins" that your fund can implement.

1.1 Cybersecurity Governance and Risk Assessments

Myth: *I will be better prepared to pass OCIE examination if I invest into technical controls, first. Once I have a better protection against cyber-threats, there is less chance of an incident.*

One of the tenets of today's cybersecurity best practice is "offense informs defense." It means that cybersecurity threats, similar to investment strategies, are not constant and continuously evolve. Whatever technology you may have in place today may not be efficient against a new threat tomorrow. That's why it is important to have proper governance and periodically evaluate the risks and gaps. This concept can be clearly seen in the SEC's approach to cybersecurity, when in September of 2015, they charged R.T. Jones Capital Equities Management with failing to adopt proper cybersecurity policies and procedures prior to a data breach. Specifically, the firm failed to:

- adopt written policies and procedures reasonably designed to safeguard customer information, and
- conduct periodic risk assessments

Quick Wins:

1. Establish an organizational body (e.g. Security & Privacy Committee) tasked with overseeing all aspects of cybersecurity and reporting information security risks, including changes in federal/local laws and regulations, directly to the Board of Directors and/or investors.
2. A Written Information Security Policy (WISP), at a minimum, should incorporate these six topics covered in the latest SEC Risk Alert.

   NOTE: We often come across firms hiring an external party to develop their WISP. I strongly recommend to first ensure that whomever is tasked with developing your WISP is indeed a subject matter expert in the SEC Cybersecurity Initiative.
3. Consider engaging a third party to conduct risk assessment / gap analysis. It will immensely help you to build the foundation for your cybersecurity program by:
   - Aligning your cybersecurity program with your strategic business plan
   - Helping you develop your cybersecurity roadmap through gap analysis
   - Using findings to develop metrics and build a business case

1.2 Access Rights and Controls

Myth: *We already have a firewall. Plus, we have enterprise-level anti-virus on all computers. All we need is to encrypt the sensitive data, so that even if someone steals it, they won't be able to use it.*

Any technical security control, e.g., a firewall, an Intrusion Prevention Systems (IPS), data encryption and many others, could be viable against some type of threats, yet defenseless against others. For example, anti-virus is known to be only 20% effective, and encryption can be circumvented under many conditions. That's exactly how the defense-in-depth methodology of layered security came about:

- No technical solution on its own can protect against evolving cyber threats. Yet, a combination of right defenses working in concert with each other will force attackers to maximize their efforts, and in turn will minimize chances of successful attacks
- Even if one layer is breached, there is time to deploy new or updated countermeasures

The defense-in-depth methodology works hand-in-hand with the CIS Critical Controls and maps well into NIST Cybersecurity Framework. It greatly helps with making the starting point.

Quick Wins:

1. **Administrative access to computer systems.** A vast majority of malware relies on having administrative access to infected system. Removing administrative privileges and only using it when required can significantly reduce the footprint of potential attacks.
2. **Access rights based on "need to know" and "least privilege" principles.** All information stored on computer systems should be protected in a way that only authorized individuals have access based on their responsibilities. For example, not all employees need the ability to modify files with sensitive information. Limiting such access can significantly reduce the damage of potential attacks or significantly lowering the risk of a data breach.

1.3 Data Loss Prevention (DLP)

Myth: *We spoke to a few vendors, and we can have DLP in no time.*

Data Loss Prevention is a strategy for controlling different types of information based on the classification. For example, proprietary information or Personally Identifiable Information (PII) may not be allowed for copying into portable media, or sent via email to external parties. There is a plethora of available DLP related products ranging in price from a few thousand to hundreds of thousands of dollars. Regardless of the price, the implementation may not be so simple, because data comes in many different forms. Most DLP products today come with predetermined policies to match specific compliance standards, such as PCI, HIPPA, SOX, etc. Most certainly, there will be a customization effort to match specific needs of your firm, which has at least two dependencies:

- DLP is a tradeoff between the convenience and security, and
- DLP customization relies on established Data Classification and Data Mapping standards

Quick Wins:

1. Establish a Data Classification policy and standards outlining the data classification types (e.g., sensitive, confidential, protected, etc.) and associated risk levels (e.g., low, medium, or high). Develop document templates (e.g., MS Office) with embedded data classification.
2. Establish dedicated, centralized locations, where different types of data must be stored.
3. Establish a strategy for these three general scenarios:
   a) Data residing on endpoint systems (workstations, portable or mobile devices)
   b) Data-at-rest on file servers, shared network storage, etc.
   c) Data-in-transit – when data is being sent via email, copied across the internet, etc.
4. Define data ownership and custodianship standards. For example, in the case of InfoHedge, we are data custodians, whereas our customers are data owners. As a data custodian, InfoHedge heavily relies on the Data Classification and Data Mapping set by our customers.

1.4 Vendor Management

Myth: *I have managed many vendors throughout my career, and I don't think this is any different.*

A spree of data breaches over the last few years, such as Target's credit card breach, originate from breached vendor networks, and then make their way into customer networks. As a result, examiners may focus on firm practices and controls related to:

- Due diligence with regard to vendor selection
- Whether vendor relationships are part of firm's ongoing risk assessment process
- Due diligence with regard to vendor access to firm's network or data, including the services provided and contractual terms related to accessing firm networks or data, and
- How vendors facilitate the mitigation of cybersecurity risks by means related to access controls, data loss prevention, and management of PII

Quick Wins:

1. Develop a technology specific Due Diligence Questionnaire (DDQ), which has been recognized in the market for its depth of content and efficiency.

1.5 Cybersecurity Awareness and Training

Myth: *We can't have our employees spending valuable time training on cybersecurity when there is plenty of cybersecurity-related information out there and we already follow the news and popular cybersecurity blogs.*

The main goal of cybersecurity training is to lower the risk of a security incident. Remember the old cliché about a chain being as strong as its weakest link? In the case of cybersecurity chain, the human happens to be the weakest link. By training your employees about cybersecurity risks, along with the consequences of taking (accepting) these risks, and different methods to avoid these risks, you eventually lower the risk of a security incident.

Quick Wins:

1. Develop short, tailored training sessions for specific job functions, based on cybersecurity risks identified for your firm and the industry
2. Encourage responsible employee and vendor behavior
3. Include procedures to follow in case of a cyber-incident

1.6 Incident Response

Myth: *Our firm has contracted a third party to provide incident response, so we don't need our own team or procedures.*

Incident Response, although technical in nature, incorporates a great deal of non-technical functions. More importantly, in order to engage incident response, you need to be aware of an incident. Nowadays, the vast majority of security incidents are reported by external parties. Similar to crisis management plans, all functions need to be clearly documented and periodically tested.

Quick Wins:

1. Determine which firm data, assets, and services warrant the most protection to help prevent attacks from causing significant harm
2. Discuss possible scenarios of security incidents with either your internal security team or another third party
3. Develop your own Incident Response Plan and procedures with assigned roles to address these scenarios. If third party services are involved, incorporate their procedures into your plan:
    - Who has the authority to engage the incident response process?
    - What is the escalation process?
    - Who will be determining the amount of actual clients' losses?
    - Who will be documenting the date/time of an incident, discovery process, escalation, and any responsive remediation efforts taken?
    - When will the investors be notified of a security incident? and,
    - When and how will this plan be tested?

CONCLUSION

The SEC Cybersecurity Initiative and NFA Cybersecurity Interpretive Notice have raised the bar on the cybersecurity awareness and preparedness, triggering prominent changes in the alternative investment industry. Fund management is expected to incorporate cybersecurity into business strategy and CapEx/OpEx budgets, as well as to develop short-term and long-term strategies on implementing adequate cybersecurity controls into every day routines.

About the Author & InfoHedge Technologies, LLC

Oleg Bogomolniy is Chief Security Officer at InfoHedge Technologies, LLC, a leader in best-in-class, single-custody IT Hosted Platform services. With expertise in security leadership, cybersecurity awareness training, forming and training of incident response teams, and digital forensics, Mr. Bogomolniy leads the InfoHedge Cybersecurity Program geared to solidify cybersecurity-aware culture of InfoHedge and promote cybersecurity awareness and compliance to InfoHedge customers as part of the vCSO® offering. To learn more about InfoHedge, please visit their website at **www.infohedge.net**.

About Richey May & Co., LLP

As a public accounting firm with hundreds of Alternative Investment clients in over 36 states, and relationships with many of the top service providers and specialists in the country, Richey May is dedicated to providing expert audit and tax services to the industry. Our team combines the dedicated expertise found in a national accounting firm with the hands-on approach to client service you'd expect from a boutique provider – a unique model that allows us to bring expert solutions and strategies to your specific business needs.

Richey May is dedicated to sharing best practices and trends in the industry - both from our advisors and from colleages in the industry - to help you stay competitive in the local and national marketplace. For more information on our firm and the services we provide, please contact **Stephen Vlasak** at **svlasak@richeymay.com**. You may also visit our website at **www.richeymay.com**.