WELLS FARGO SECURITIES

# Cybersecurity preparedness

## *Combating today's threats*

*Wendy Beer, Head of Business Consulting, Wells Fargo Prime Services*

*Alternative asset managers are faced with increasing challenges in today's threat landscape and must be progressively diligent in protecting their firm's assets and infrastructure. Thoughtful cyber planning incorporating operational and technological infrastructures as well as regulatory considerations are vital to combatting cyber-attacks.*

The follow is a summary from Wells Fargo Prime Services' *On The Horizon* conference series held on December 9, 2015 featuring:

- Eldon Sprickerhoff, Founder & Chief Security Strategist, eSentire
- Stuart Levi, Partner, New York, Skadden, Arps, Slate, Meagher & Flom LLP
- Vinod Paul, Managing Director, Services & Business Development, Eze Castle Integration, Inc.
- Timothy O'Brien, Supervisory Special Agent, Cyber branch, Federal Bureau of Investigation – New York Office
- Marc P. Berger, Partner, Government Enforcement, Ropes & Gray LLP

## The current landscape

Marc Berger's opening statements emphasized the extent of the cybersecurity threat currently facing firms across a wide swath of industries. He quoted FBI Director James Comey, who stated that, "There are two kinds of big companies in the United States. There are those who've been hacked ... and those who don't know they've been hacked ...." (FBI Director James B. Comey, 60 Minutes, CBS TV Interview, October 5, 2014).

Alarming statistics from the Ponemon Institute's 2015 Cost of Cyber Crime Study, conducted with HP Enterprise Security, found that the average cost to resolve a single cybersecurity incident is $1.9M, and the average time to resolve is 46 days. Perpetrators range from nation-state-sponsored hackers, disgruntled/rogue employees, organized crime, activists, and other thieves.

*"There are two kinds of big companies in the United States. There are those who've been hacked ... and those who don't know they've been hacked...."*

*- FBI Director James B. Comey, 60 Minutes, CBS TV Interview, October5, 2014*

According to the Breach Report issued January 12, 2015 by the Identity Theft Resource Center ("ITRC"), there were 783 data breaches in 2014, an increase of 27.5% over 2013 and a record high overall.

The most commonly breached industries were: medical/healthcare (42.5%), business (33.0%), government/military (11.7%), and, in fifth, banking/credit, financial (5.5%).

As of June 30, 2015, per ITRC data, in 2015 the banking industry experienced an increase of 85% versus 2014 data for the same period. Thus far in 2015, per ITRC data, banking/credit/financial businesses have experienced 60 breaches, or 9.5% of the total. Cyber-attacks carried out on the financial community have almost doubled in 2015, and industry experts believe these numbers will continue to increase unless adequate precautions and prevention measures are taken.

Timothy O'Brien highlighted that people want to access or attack data of financial institutions and asset managers for a number of reasons, including:

- Fraud/identify theft
- Espionage (nation states/advanced persistent threat, terrorists)
- Insider sabotage or theft (disgruntled/rogue employees)
- Hacktivism (motivated by political motives/activists)

## Cybersecurity has become an increasing regulatory focus

### Regulatory Expectations

Stuart Levi noted that when an Alternative asset manager ("AAM") suffers a cyberattack, it may find itself in a unique position with its regulators. On one hand, it is the victim, and will expect to be treated as such by regulators. Generally, this is the way that the FBI and law enforcement views a firm in these situations.

However, regulators may also be looking at whether enforcement action is warranted if the AAM failed to implement appropriate security measures that would have prevented the attack from occurring. For example, the SEC recently brought enforcement action because a firm "did not have the required cybersecurity policies and procedures reasonably designed to protect customer records and information in advance of a breach, thus violating the safeguards rule." This action was brought even though "there was no apparent financial harm to clients" (SEC vs. R.T. Jones Capital Equities Management, September 22, 2015.)

The clear message from all regulators is that all financial institutions, including AAMs, need to anticipate potential cybersecurity events, implement appropriate safeguards, and have clear cyber-response procedures in place before an incident occurs. Waiting to react once a breach occurs may result in an enforcement action.

### Third Party Vendor Relationships

Where there is reliance on third party service providers, the AAM is **NOT** relieved of its cybersecurity risks but rather, has the obligation to assess and monitor the provider's security policies and procedures and conduct adequate due diligence. As outlined in the panel, steps necessary to fulfill an AAM's obligations around vendor management include:

- Understand the breadth/depth of the relationships your firm has established
- Calculate potential risks and vulnerabilities
- Conduct thorough due diligence before the relationship commences
- Continue conducting proper due diligence throughout the course of the relationship
- Employ contingency plans for terminating vendor contracts
- Create a plan of action in the instance of a security breach

### What do regulators want to see in terms of cyber risk preparedness?

Stuart Levi noted that there are six themes that regulators tend to focus on when they provide guidance on cybersecurity, and that every AAM should consider:

1. Periodic Cybersecurity Risk Assessments
2. Governance
3. Training
4. Access Control
5. Vendor Management
6. Information Sharing
7. A Security Incident Response Plan ("SIRP") that is in addition to any Business Continuity Plan the firm may have. A SIRP should set forth the firm's procedures in the event of an attack, including who will be part of the team and the firm's disclosure obligations

Finally, firms should consider purchasing Cybersecurity Insurance Coverage. While many firms believe that they are already covered under their General Commercial Liability or property policies, the reality is that many of these policies explicitly carve out breaches.

Cybersecurity insurance can cover a number of areas, including: network security, data breach, network extortion, business interruption and digital asset loss. Specific cyber liability insurance will help mitigate costs during a breach. Some of the coverages that can be included in a policy are:

- If it is a cyber-extortion situation, the insurer can provide services to deal with ransom demands
- Assistance with notification of investors and employees of the breach
- Hire crisis management services to help with media and public perception to help minimize the reputational risk
- Determine if there was any business interruption and lost revenue as a result of the breach
- Assess the damage to your systems and repair them as quickly as possible

*The average cost to resolve a single cybersecurity incident is $1.9M, and the average time to resolve is 46 days*

*- Ponemon Institute's 2015 Cost of Cyber Crime Study, conducted with HP Enterprise Security*

### How do you know what is the appropriate amount of readiness given your AUM?

While the SEC has issued various risk alerts providing guidance on areas of focus, the guidance and rules are not prescriptive. As a result, firms are challenged to understand what level of cyber-security readiness will be deemed sufficient to meet regulatory obligations given their AUM.

Responding to this ambiguity, and since there cannot be a "one size fits all" approach to cyber security, eSentire created a matrix to assist AAMs to determine what would be considered a pragmatic and sensible approach to

cyber-security, while also taking into account the firm's AUM. While not explicitly or tacitly approved by any regulators, this matrix offers a helpful framework for understanding compliance with each of the SEC's cybersecurity recommendations and an easy to follow "To-Do" List.

## Conclusion

***Cybersecurity readiness may become a competitive advantage.***

According to the Ponemon Institute's 2015 Global Megatrends in Cybersecurity, sponsored by Raytheon, 25% of respondents in a study say C-level executives currently view cybersecurity as a competitive advantage, versus 59% who say it will be a competitive advantage three years from now. Other points of note from this survey:

- 66% strongly agree that "My organization needs more knowledgeable and experienced cybersecurity practitioners."
- Only 39% agree that their organization has ample resources to ensure all cybersecurity requirements are met."

Information Sharing is an evolving theme. In an industry historically known for protecting its information, recent regulatory developments may foster a change in how firms think about sharing information. Highlighting the importance of information sharing, on December 19, 2015, after years of failing to enact cyber threat information-sharing legislation, Congress passed the controversial Cybersecurity Information-Sharing Act of 2015.

Firms can no longer act in silos, but must share information with industry peers (including competitors) to protect the entire sector. AAM's can expect to see investors placing greater emphasis on cybersecurity as a part of its due diligence, and regulators focusing on cybersecurity in their routine regulatory exams.

---

*"Investors and customers deserve a clear understanding of whether public companies are prioritizing cybersecurity and whether they have directors who can play an effective role in cybersecurity risk oversight,"*

*- U.S. Senator, Jack Reed, RI*

---

## About *On The Horizon* conference series

As markets move and regulations change, alternative asset managers need to remain at the forefront of issues. Our Business Consulting group hosts "On The Horizon", a regular morning conference series, where key industry experts discuss vanguard topics specifically effecting alternative asset managers.

### About Wells Fargo Prime Services

Part of the Institutional Investor Services group, Wells Fargo Prime Services offers comprehensive prime brokerage services and solutions for alternative asset managers. Through our multi-asset class platform, we help managers meet their operational and financial goals with:

- Integrated financing solutions
- Technology and operational solutions
- Capital introductions
- Business consulting services
- Risk management solutions

### About the Business Consulting group

The Business Consulting group delivers subject matter expertise for alternative asset managers including: business development (from launch to franchise management), best practices, peer analysis and benchmarking, and thought leadership.

We help fund managers focus on their day-to-day investment objectives and improve the efficiency of their operations. By leveraging our knowledge of industry service providers we facilitate key introductions and discussions to achieve the right operational fit for our customers' business. We offer subject matter expertise across the full spectrum of hedge fund operations including formation and structure, strategic growth, trading workflows, and technology platforms.

To learn more about our thought leadership initiatives:

**Wendy Beer**
Head of Business Consulting
(212) 822-8731
Wendy.Beer@wellsfargo.com

wellsfargo.com/primeservices

## Appendix/Resources

OCIE Cybersecurity Risk Alert April 15, 2014
http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf

SEC Division of Investment Management Cyber Security Guidance, April 2015
http://www.sec.gov/investment/im-guidance-2015-02.pdf

SEC Cybersecurity Examination Sweep Summary, February 3, 2015
http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf

Hedge Fund Standards Board Toolbox Series, September 2015
http://www.hfsb.org/?page=13064

### Cyber Liability Insurance

Claudia J. Ramone
Vice President of Sales
Maloy Risk Services
(646) 722-9395
cramone@maloyrs.com
Linkedin: claudiaramone

David A. Parker
Partner President Employee Benefits
Assured SKCG, Inc.
(914) 761-9000 ext: 5004
dparker@skcg.com
www.skcg.com