BILLED AS: IN HOUSE PERSPECTIVE:

Discuss regulators and how they are making the requirements more rigorous. Review of FINRA and other agencies policies and how should a company prepare?

What are the major implications for Financial Institutions of the intense focus by the regulators on cybersecurity?

Thank you Megan

After years of regulatory reform the Financial Services Industry is experiencing a noticeable shift in Regulatory focus away from improving financial strength to **governance, structure, and operations concerns.**

Probably the best example of Regulator focus on governance, structure and operations is their approach to Cybersecurity.

Virtually every regulatory body in the Financial Services world has increased their regulation related to cybersecurity and increased the intensity of their examinations over cybersecurity controls over the last five years.

- In February this year, **FINRA**, the SRO for broker / dealers, published a 50 page report on cybersecurity practices. This document is both a review of current practices and a guide for broker dealers in establishing their cyber security infrastructure. It's quite good and is available on their website. I recommend reading it.

- In the SEC world, the **Investment Management Division** earlier in 2015 highlighted the cybersecurity of Registered Investment Companies ("funds") and Registered Investment Advisers ("advisers") as a critical risk issue. Clearly, both Funds and RIA's need to protect confidential and sensitive information from third parties, that they receive in executing these activities. Because of the rapidly changing nature of cyber threats, the Division will continue its focus on cybersecurity and monitor cyber-related events in this area, especially breaches.

- All of the **Federal Bank Regulators**, including the Federal Reserve, the OCC and the FDIC have issued cybersecurity regulations and guidance, and have intensified their regulatory focus and scrutiny over cybersecurity.

BILLED AS: IN HOUSE PERSPECTIVE:

Discuss regulators and how they are making the requirements more rigorous. Review of FINRA and other agencies policies and how should a company prepare?

- And of course the **New York State Department of Financial Services** has taken an aggressive tac driven by outgoing Superintendent Benjamin Lawsky. As part of this initiative the Superintendent has directed his Head of the NY Capital Markets Division to issue a letter to CEO's, General Council's Tech Heads. The letter states that: "In an effort to promote greater cyber security across the financial services industry, the New York State Department of Financial Servicesv v plans to expand its IT examination procedures to **view cyber security as an integral aspect of their overall risk management strategy"**

None of this is new to anyone in the audience today. And it is not necessary for me to go into any depth as to why this increase regulatory focus is happening, given the widespread publication of major cybersecurity breaches, and the losses they have caused. The good news is that the financial services industry, even with the noted losses of JP MorganChase and others, is in better shape than most industries. The healthcare industry, whose records are valuable to cyber thieves, is estimated to be 10 years behind the financial services industry in cybersecurity. This comparison is an interesting notion and may give some of us a moment of self-congratulation, but this does not in any real way reduce the cyber risks that we face.

The key takeaway here is that cyber not only creates all the risks that my colleagues will talk about, but it now creates important Regulatory Risks.

BILLED AS: IN HOUSE PERSPECTIVE:

Discuss regulators and how they are making the requirements more rigorous. Review of FINRA and other agencies policies and how should a company prepare?

What are some of the major challenges, regulatory and other, encountered by your clients in establishing Cybersecurity programs? Are there any common pitfalls in this implementation?

A. Virtually every financial institution has begun to deal with the very real cybersecurity risks that we all face, and frankly, cybersecurity consultants abound. A Google search for "cybersecurity consultants" yielded about 100 hits, my favorite hit was "HourlyNerd.com."

B. There are good examples and not-so good examples out there. My first example is where the FI fell short in its cybersecurity implementation. The financial institution in this instance engaged a world class Cybersecurity firm to establish a comprehensive "Defense in Depth" over its other programs. The program included 1.) BOD & Management training, 2.) advanced assessment of the institution, and its vendors and customers, as well as assistance in creating an enhanced partnership between risk managers and IT.

Unfortunately, this FI thought they had done enough with phase 1.), and never implemented phase 2.). Clearly the training is critical, and these steps might even satisfy some regulators, but it left the institution with huge cyber risks.

C. In a more positive example, one of my banking clients engaged a cybersecurity consulting firm with global experience to design and implement their cybersecurity program, including the BOD, Management, and staff training, 2.) advanced assessment of the institution, and its vendors and customers. And then they went the extra step of hiring the consulting firm to run a 3.) continuous monitoring Program. Continuous monitoring provides strength and depth to the FI's cybersecurity program by running advanced assess processes quarterly.

The takeaway here is that cybersecurity program design *and* execution of implementation matter.

BILLED AS: IN HOUSE PERSPECTIVE:

Discuss regulators and how they are making the requirements more rigorous. Review of FINRA and other agencies policies and how should a company prepare?

What are the attributes that you have seen, in the Financial Institutions space, of successful models for the implementation Cybersecurity programs? Is there any regulatory guidance for implementation?

A. As I mentioned earlier, in February of 2015 FINRA released its "Report on Cybersecurity Practices." It sets an extremely high bar for B/D's in setting up and managing their cybersecurity. FINRA talks about eight cybersecurity areas that it considers important. These areas are: 1.) Governance, 2.) Risk Assessment, 3.) Technical Controls, 4.) Incident Response Planning, 5.) Vendor Management, 6.) Staff Training, 7.) Cyber Intelligence and Information Sharing, and 8.) Cyber insurance. All of these areas are important; I will discuss five of them.

B.

C. A critical area, among many critical areas is **Vendor management**: Vendors have access to their FI partner's systems and data bases. As recent incidents have shown, vendors can be a significant source of cybersecurity risk. These risks can arise in different ways. For example, if a vendor or one of its employees can misuses FI's data or systems. Additionally, if the vendor itself is subject to a cyberattack it may compromises Firm systems or Firm data. Said differently, an attack on a vendor becomes a vector for an attack on a Firm's systems. FI's need an effective vendor management program in place to help guard against these risks.

D. **Incident Response**: An incident response plan charters a dedicated Cyber Security Incident Response Team to address all the possible attack vectors and take the legitimate concerns of third parties into account. The primary objective of an incident response plan is to provide a framework to manage a cybersecurity event or incident in a way that limits damage

D Cybersecurity training needs and requirements from the must start from BOD on down through the organization. Employees are one of the major sources of cybersecurity risk for firms. FINRA found that many of the cybersecurity attacks that firms identified were successful precisely because employees made mistakes, such as inadvertently downloading

malware or responding to a phishing attack. For this reason, cybersecurity training is an essential component of any cybersecurity program.

E. **Cyber Insurance**: Coverage is now offered by many major insurance underwriters as most commercial policies do not over cyber relate losses. This is a rapidly evolving segment of the insurance market. It is estimated that premiums written for cyber insurance were $1B in 2014 and may grow to $2B in 2015. In order to obtain cyber insurance, a company, must have the minimum level of cybersecurity controls set by each insurance company. Further, even if insurance can be obtained the premium level will depend on the underwriter's evaluation of those controls. And most importantly, we have seen cyber insurance claims denied if the controls are not maintained and functioning to the level required by the insurance company.

BILLED AS: IN HOUSE PERSPECTIVE:

Discuss regulators and how they are making the requirements more rigorous. Review of FINRA and other agencies policies and how should a company prepare?

What do you see as the one overriding key to successful implementation of a Cybersecurity program that meets relevant regulatory criteria?

Having described the Regulatory landscape which is increasingly, and critically, focused on Cybersecurity, and having outlined some real life examples, good and bad, of how financial institutions are dealing with Cyber related risks, I am going to turn the page and discuss a critical way of thinking about cyber risks and an approach that is required by virtually every regulator that I have referred to.

This strongest, the most successful, approach to shield financial institutions against cyber risks is to embed all cybersecurity functions in the Enterprise Risk Management process, or ERM, sometimes referred to as corporate risk governance. I am sure that you all are familiar with ERM as it was brought into widespread acceptance with the issuance of the COSO internal control frame work ten years ago. COSO defined ERM as: *"… a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."*

Interestingly, while most financial institutions are still working on their ERM implementation, COSO has engaged PwC to re-write its 2004 ERM. The main drivers of this re-write are increase reliance on technology and the regulatory emphasis ERM. Prior the advent of ERM financial institutions manage their risks in the traditional categories: credit, ALCO, Operations, Technology, regulatory, legal, etc. Clearly, managing these risks in one

integrated ERM framework has proved more effective than the old silo approach.

Cybersecurity **is the newest risk area to join the list above**. Because of its nature as a risk area that touches virtually every area of a financial institution, Cybersecurity can only be addressed by an institution-wide ERM approach.

There are four key take-aways that I want you to think about:

1. **Training and creation of a cyber risk awareness culture are critical**
2. **In the technical, assessment levels, all vectors must be addressed. Ways that strengthen technical defenses are:**

a. **Continuous monitoring, and**
b. **Using a multiple layer approach**

3. **Learn about and add cyber insurance to your cyber defenses,**
4. **Overall, use a Corporate Governance, ERM approach**