The NIST Cybersecurity Framework – Encouraging NIST Adoption Via Cost/Benefit Analysis

Paul A. Ferrillo

The NIST Cybersecurity Framework – Encouraging NIST Adoption Via Cost Benefit Analysis

- Until the President's Cybersecurity Summit at Stanford University last month, the public profile of the NIST cybersecurity framework was not enormous.
  - Cyber is "scary" for directors.
  - Not a lot of public "adopters."
  - Cyber is not intuitive like FASB rules, which have been around for years.
  - CISO's and CIO's tend to be silo driven – Common refrain from CISO's, "We are doing it my way, and its worked for the last few years without a problem."

The NIST Cybersecurity Framework – Encouraging NIST Adoption Via Cost Benefit Analysis continued

- We have had a different experience rolling the Framework out to boards of directors, *i.e.* the ultimate decision-makers/fiduciaries of a public or private company.
- Our “top down” approach is based upon logic, reason, current events and a cost/benefit analysis.
- Most of all, it is based on the concept of fiduciary duty and the concept of enterprise risk management. The board’s job is cyber security risk oversight.
- Because boards need more and better laser – pointed guidance, they need the NIST cybersecurity framework.

The NIST Cybersecurity Framework – Encouraging NIST Adoption Via Cost Benefit Analysis continued

- Adoption of NIST as an industry best practice means:
  - Showing “you are paying attention” to cybersecurity in general.
  - Showing the regulators “you are paying attention”.
  - Showing your customers “you are paying attention”.
  - Showing your shareholder/investors and the financial markets that “you are paying attention”.
  - Showing the plaintiffs bar that “you are paying attention” to cybersecurity by having NIST-based discussions
  - NIST is “one stop shopping” if embraced by regulators seeking to restore customer confidence, investor protection and market stability in the face of cyber terrorism, hacktivism and cyber crime.

The NIST Cybersecurity Framework – Encouraging NIST Adoption Via Cost Benefit Analysis continued

- What is the new “core curriculum” of cybersecurity?
  - The fiasco of having to pay potentially limitless costs to remediate a cyber breach versus the preventive costs associated with improving the company’s cybersecurity posture.
  - By any stretch of the imagination, this equation should generate a “high positive” number indicating the NIST cybersecurity framework is a net positive investment.

The NIST Cybersecurity Framework – Key Principles for Boards of Directors

Weil

- Perception at companies does not equal reality
  - Ninety percent of companies believe they are not vulnerable to hackers, despite over half experiencing a "security incident" over the last 12 months.
  - Out of the total respondents participating in the survey, 88 percent claimed they were somewhat or very confident that they were safeguarded from external cyber threats. This number increased to 92 percent when only questioning technology sector respondents. Over 60 percent of total participants assessed their ability to alleviate newly developed threats as either average or high. [Deloitte 2013 study]

The NIST Cybersecurity Framework – Key Principles for Boards of Directors continued

- The truth
  - "OTA's analysis of nearly 500 breaches reported in the first half of 2014 revealed upwards of 90% could have been avoided had simple controls and security best practices been implemented. As the dependency on outsourcing and the cloud has increased, businesses are increasingly relying on service providers to keep their data secure and abide by their privacy policies, further highlighting the need to develop comprehensive security controls and practices." [Online Trust Alliance 2015 report] [emphasis added]

The NIST Cybersecurity Framework – Rollout and Implementation Strategies

Weil

- Today, there is a new normal:
- A “Cybercrime Economy” that if allowed to proceed unimpeded will cost companies hundreds of millions of dollars [and U.S. economy hundreds of billions of dollars] to repair and remediate cybersecurity breaches, let alone repair the loss of reputation, investor confidence and goodwill.

The NIST Cybersecurity Framework – Rollout and Implementation Strategies continued

- "We are concerned that within the next decade, or perhaps sooner, we will experience an Armageddon-type cyber event that causes a significant disruption in the financial system for a period of time," said Benjamin Lawsky, head of the NY Dept. of Financial Services on Wednesday March 6, 2014 in a speech at Columbia Law School.

The NIST Cybersecurity Framework – Rollout and Implementation Strategies continued

Weil

- The fiduciary duties of corporate directors include enterprise risk management, and that covers cyber security oversight.
- Questions that should be asked: "What is our risk from a cyber perspective?" "What is our risk appetite?" "How can we mitigate our risk, or transfer it to a third party through insurance?" and "What can we do better to protect our most valuable IP assets?"
- Basic questions to ask and answer. It's a director's duty to ask and answer them regardless.
- The self-evident conclusion -- Lost "opportunity" cost to implement NIST-based cyber security discussions = ZERO.

The NIST Cybersecurity Framework – Rollout and Implementation Strategies continued

Weil

- C-Suite and CISO discussions implementing cyber security spending decisions:
  - Steps towards improving cybersecurity posture less susceptible to getting lost in “budgetary process,” if approved by the board in advance;
  - Most companies not starting from scratch – incremental improvements versus major improvements = cost/benefit analysis per se.
  - For companies starting from scratch = cost to implement will be higher but yet if you can’t implement good cybersecurity, why bother? Good cybersecurity must be part of the DNA of the Company. It is the ultimate team sport.

The NIST Cybersecurity Framework – Rollout and Implementation Strategies continued

- Elements of Risk and Cost to be Considered if nothing is done to improve my security posture:
  - Clean up – forensic and business continuity costs
  - Lost customers
  - Lost reputation/lost opportunity cost and loss of goodwill
  - Lost investors/loss of investment opportunities
  - Regulatory scrutiny/investigations/proceedings
  - Customer and Bank class actions alleging failure to meet minimum cybersecurity "standards" offered by NIST compliance (*See e.g.* Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis, Indiana U. 2015)
  - Loss of Enterprise Value = Shareholder class and derivative actions alleging oversight failure
  - Loss of future investors/withdrawal of capital post-breach

The NIST Cybersecurity Framework – Rollout and Implementation Strategies continued

Weil

- Proposed budgetary cost of improvements to begin addressing cybersecurity posture -- calculated at a minimum of $500,000 (implementing NIST framework (including internal company hours)), plus cost of instituting a company-wide anti-spear phishing program, plus basic cost of 128 bit encryption technology.
- So what are the potential costs to the company of not making the suggested improvements to their company's cybersecurity posture?
- Bottom – Line: Its cheaper to make these minimum cybersecurity improvements through adopting NIST then waiting for something bad to happen to the Company.

The NIST Cybersecurity Framework – The Carnage of a Major Cyber Attack

Weil

- Target – Cost to clean up as of last quarter – $283 million (before insurance recovery), not including 140 class action suits – Est. $1 billion in costs when all “cleaned up”.
- Home Depot – cost to clean up as of last quarter – $43 million, not including 44 class actions.
- Sony Pictures – est. $35 million to date.
- Anthem – estimated to be well in excess of $100 million to clean up, plus approximately 40 class action lawsuits to date.
- More generally, loss of $195 per record stolen in U.S. (Ponemon cost of data breach report)

The NIST Cybersecurity Framework – The Carnage of a Major Cyber Attack continued

Weil

- Infrastructure Losses – corrupted servers and hard drives – Las Vegas Sands (est. $100 million in losses) and Sony.
- Loss of reputation – foot traffic – Target 43% decrease in profits in 4Q 2013 – Q1 2014 net earnings down 16% – measurable brand damage post-attack.
- Loss of market capitalization if investors get angry – $10 billion market capitalization loss upon market reflection of breach, causing both securities class action and derivative action.
- Same sort of analysis should hold true for other industry segments – e.g. PE, HF.

The NIST Cybersecurity Framework – Rollout and Implementation Strategies

Weil

- Whether you are a big company or small company its cheaper to do something rather than “stick you head in the sand.”
- The costs to smaller companies can be equally and potentially catastrophic because their balance sheets cannot sustain a large clean up cost or a “run on the bank.” Customers or investors just pull out and “shop” or “invest” somewhere else;
- Unless the company was prepared enough to buy cyber insurance….

The NIST Cybersecurity Framework – Rollout and Implementation Strategies continued

- But the cyber insurance market has dramatically changed over the last eight months post JPM, Home Depot, Sony Pictures and Anthem breaches;
- Underwriting and pricing has gotten much tougher.
- Many companies (*e.g.* AIG) have now started using the Framework as a "benchmark" upon which to assess the cybersecurity posture of a potential insured, using the same discussions we ourselves might have with a board, creating additional synergy and purpose to adopting the Framework.
- Several cyber insurers have either pulled out, or pulled back from market or market segments given claims experiences in last six months.

The NIST Cybersecurity Framework – Rollout and Implementation Strategies continued

- If the insurer does not get good answers to its NIST-based questions:
  - Higher premiums – up to 4x recently
  - Higher retentions/deductibles
  - Or maybe even no coverage offered at all if the insurer is not satisfied that the company is paying attention to cybersecurity detail.

The NIST Cybersecurity Framework – Not a Silver Bullet, But a Protector of Enterprise Value

Weil

- ERM and cybersecurity are board oversight fiduciary duties. Period. No changing that fact.
- Adoption of the Framework fosters and encourages discussions allowing directors and officers to fulfill their fiduciary duties regarding cybersecurity oversight by, among other things, aligning “risk” with Company resources.
- Adoption of the Framework may improve a company’s cost-effective access to the cyberinsurance market, which Corporate America desperately needs today.
- Today, there really is no excuse to “do nothing.”

"THE AMERICAN DREAM IS STILL ALIVE OUT THERE, AND HARD WORK WILL GET YOU THERE. YOU DON'T NECESSARILY NEED TO HAVE AN IVY LEAGUE EDUCATION OR TO HAVE MILLIONS OF DOLLARS STARTUP MONEY. IT CAN BE DONE WITH AN IDEA, HARD WORK AND DETERMINATION."

BILL RANCIC

Lifehack Quotes

The NIST Cybersecurity Framework – Not a Silver Bullet, But a Protector of Enterprise Value continued

- For any questions or comments, contact:

Paul A. Ferrillo, Esq.
Weil Gotshal & Manges LLP
212 – 310-8372
paul.ferrillo@weil.com