January 2012

Warning: Cyber Liability Ahead! Navigating the SEC's Guidance

By Lauri Floresca, *Senior Vice President, Corporate and Executive Protection*

The SEC offers timely guidance on cybersecurity disclosures – but how difficult is it to take their advice? And just what is this "relevant insurance coverage" they suggest you disclose?

In October 2011, the SEC published informal guidance to issuers regarding disclosure obligations relating to cybersecurity risks. It's no surprise the SEC is spotlighting this issue at this time: with high profile cybersecurity events at companies like Sony, RSA Security, CitiGroup, and even the New York Yankees, 2011 was labeled "The Year of the Breach" by many cyber liability experts.

The SEC's guidance suggests that in determining whether to add disclosure on cyber liability to their risk factors, companies should consider (1) the "probability of cyber incidents occurring" and (2) "the quantitative and qualitative magnitude of those risks." The SEC also tells companies that appropriate disclosure may include a "description of relevant insurance coverage."

Breaches in the News

Epsilon (March 2011)
Breach of the database for the world's largest e-mail vendor, exposed dozens of major companies and their clients to phishing attacks.

RSA Security (March 2011)
Hackers used social engineering to imbed a virus that would ultimately grant them access to critical info about RSA's Secure Access Tokens.

Sony (April 2011)
Hackers accessed personal data for more than 100 million users of Sony's online games. Over 55 suits filed in the US along with investigations by state and federal regulators.

CitiGroup (May 2011)
Hackers obtained personal data on approximately 1% of Citibank's 21 million users. At least 3.400 customers were affected with losses totaling $2.7M.

Sega (June 2011)
Japanese video game developer had data belonging to 1.3 million of their customers stolen from its database.

Morgan Stanley (July 2011)
Personal information belonging to 34,000 investment clients was lost and possibly stolen.

Lincoln Financial Group (August 2011)
Names and Social Security numbers of over 90,000 retirement plan enrollees were exposed by a data base programming error.

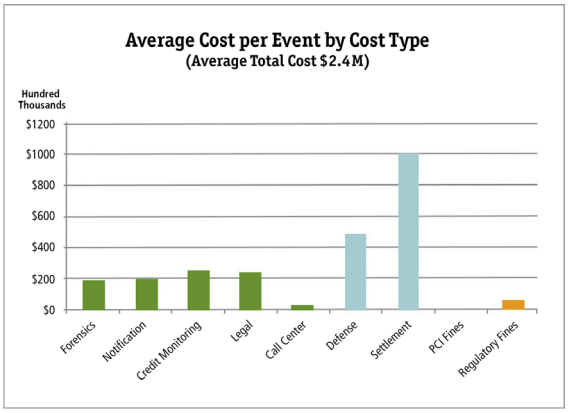
Probability? Perhaps 100%

Cyber security experts suggest that the answer to the first question on probability is something close to 100%. A June 2011 survey by Ponemon Research of IT professionals at 583 U.S. companies of varying sizes found that 90% had experienced a breach in the last twelve months. And in discussing a widespread cyber espionage campaign known as "Operation Shady RAT (Remote Access Tool)," McAfee researcher Dmitri Alperovitch said, "I divide the entire set of Fortune 2000 firms into two categories: those that know they've been compromised and those that don't know yet."

Assessing the magnitude of that risk is more difficult. With few exceptions, all companies now rely on computer networks, both internal and external, for ever-increasing aspects of their business. Companies offering services or selling goods online clearly depend on the availability of their websites and their ability to execute immediate transactions to sustain revenue growth. In addition, many companies that do not offer their products or services online still rely upon the integrity of their networks, and the data stored on them. All organizations need to consider both the immediate costs and loss of revenue from a security breach as well as the potential reputational damage.

Data Breach Costs

Some of the most significant costs of a security breach are those involved with the loss of personal data. Forty-six states currently require companies to notify individuals when their personally-identifiable information (PII) has been exposed. Generally, these laws concern data that includes some combination of identifying information (name, address, etc.) with confidential information (account number and password, social security number, medical information, etc.).



Source: NetDiligence®, "Cyber Liability & Data Breach Insurance Claims," June 2011

In addition to the cost of notifying customers of the potential exposure, companies may find it necessary to offer credit monitoring services if it is reasonably likely that the data has been accessed by third parties. More stringent requirements also come into play for companies storing health or financial data. Even if not required, offering credit monitoring or identity theft services to affected customers might deter lawsuits, reducing ultimate liability costs for the breach.

The costs associated with a data breach can be staggering. A 2010 study by the Ponemon Institute found that the aggregate cost of a data breach was $214 per record. That figure includes loss of revenue and reputational costs, which can be very difficult to quantify. But a 2011 study by NetDiligence, a cybersecurity risk management company, cited the average insurable cost of a data breach at $2.4M. This figure includes the real costs paid by insurance carriers under "Cyber Liability" policies for forensics, legal research, breach notification services, and defense and settlement for litigation resulting from the breach.

Know Your Insurance

Understanding the risk is one challenge, but the SEC's guidance adds another wrinkle. The SEC suggests that it may be appropriate for companies to include a description of "relevant insurance coverage." This simple statement is in fact, quite complex. Many different types of insurance policies may come into play to address cyber liability exposures, and all of them have coverage limitations. As a result, providing investors with a succinct summary of insurance that is also accurate will be challenging.

The SEC's guidance lists categories of costs that companies should consider in assessing their cyber liability. This is difficult to reconcile with their recommendation to disclose relevant insurance, as the availability of coverage for these costs varies significantly:

- Remediation costs– *some costs insurable, sublimits often apply*
- Increased cyber security protection costs – *not generally insurable*
- Lost revenues resulting from a cyber attack – *insurable, significant limitations/waiting periods apply*
- Litigation – *insurable*
- Reputational damage – *specialized insurance products available, limited in scope*

POTENTIAL CYBER LIABILITY COVERAGE COMPONENTS

DIRECT/FIRST PARTY COSTS*

- Crisis Management
  - – Forensic
  - – Legal
    - – Public Relations
- Notification Costs
- Credit Monitoring
- Business Interruption
- Data Replacement
- Cyber Extortion

INDIRECT/THIRD-PARTY COSTS

- Customer/Consumer Suits
  - – Defense
  - – Settlements
- Regulatory*
  - – Defense
  - – Fines
  - – Penalties
- Charges levied by credit card issuers
- PCI-DSS fines and assessments*

*sub-limits typically apply

Seeking coverage for this growing area of liability, many companies have started to purchase policies referred to as "Cyber Liability", "Technology E&O", or "Privacy & Security Liability." These contracts are not standardized, however, and the policy forms offered are rapidly evolving. Moreover, a maze of sublimits can make it difficult to ensure that coverage will be sufficient for a large breach. These policies may also combine coverage for traditional E&O claims, media liability, intellectual property infringement, and network security/privacy breaches into a single contract. The range of available coverage is significant, and companies need to work with their insurance brokers and other outside advisors to put together a cyber liability program tailored to an organization's needs.

Does a Company Really Need Separate Cyber Coverage?

Some coverage attorneys have opined that a basic General Liability (GL) policy may well cover some of the third party liability associated with a breach. This may have been possible in the past, but in recent years insurers have been modifying GL policies to reduce or exclude coverage for this new area of claims. In the current GL insurance market, most policies do not treat "data" as tangible property, and as such would not treat a data breach as property damage to trigger coverage. In addition, most GL contracts have been modified for technology companies (and firms conducting business online) to exclude personal injury claims, including those that involve violations of privacy laws. As a result, a GL policy is unlikely to respond to the third party liability for a breach, let alone the immediate (and significant) first party costs of forensics and compliance with privacy breach notification laws.

These coverage obstacles have been spotlighted in the 2011 Sony Playstation Network breach. Sony's insurer, Zurich, has asked the New York Supreme Court to confirm that its GL policy has no obligation to respond to the breach claims against Sony which include more than 50 class-action lawsuits (a December 29, 2010 article in the *New York Times* noted that Sony does maintain cyber liability insurance policies which will cover "significant portions" of the liability from the data breach).

For most companies, the best solution is likely to be a comprehensive cyber liability policy that addresses both the direct (first party) and indirect (third party) costs of responding to a breach event. To implement such a program, the first step involves a review of your specific business and security practices to assess the potential cyber liability exposure. We've included here a sample list of questions to consider as a starting point, but for more information on cyber risk analysis and cyber liability insurance, contact Lauri Floresca at lfloresca@wsandco.com.

CHECKLIST FOR EXECUTIVES

DATA

- What kind of data do we collect? What is stored and for how long?
- Other than employee records, do we collect any Personally Identifiable Information ("PII") or Personal Health Information ("PHI")?
- Do we encrypt that data? At rest and in transit? On mobile devices?
- Do we have a data breach response plan?

VENDORS

- Do we use third party vendors to store or process information?
- What indemnity rights or limitations on liability exist in the contracts with those vendors?
- Who will be responsible for notifying customers in the event of a data breach?

RISK TRANSFER

- Do we purchase Cyber Liability insurance that includes coverage for our costs to comply with privacy breach notification laws?
- What limit of liability do we carry and what sublimits apply?