ANDERSON KILL
ATTORNEYS AND COUNSELORS AT LAW

This article was originally published by Banking Exchange on May 15, 2017

N.Y. CYBERSECURITY RULES DRIVE INSURANCE REVIEWS

Potential national model suggests need for checking your cyber coverage

By: Robert D. Chesler and Marc D. Schein*

Do IT experts and senior managers have a "failure to communicate"?

Earlier this year, the Ponemon Institute issued the research report, *The Cost & Consequences of Security Complexity* [registration required]. One of the report's findings is that the growing complexity of the security technology world has resulted in "difficulty in communicating the organization's security strategy and approach to deal with cyber threats to senior management." Of the IT specialists Ponemon polled, 67% agreed that their companies' approach to dealing with cyber threats "is too complex to explain to senior executives."

This goes against the grain. Senior executives understand tax implications, although they are not accossmallsuntants. Senior executives deal with complex legal matters on a daily basis, though they did not graduate law school.

So why is it, when senior executives are faced with cyber security issues, employees, service providers, and in-house IT personnel have such a hard time explaining the strategy being implemented to protect the crown jewels of the business? These include such essential factors as the personally identifiable information (PII) of their clients, employees, and vendors; payment card information of clients (PCI); and even protected health information (PHI) of employees.

This is a timely question because a New York development that could spark activity in other states underscores how important it is for senior management to "get" cyber security—and the insurance coverage that protects companies when cyber threats become incidents.

New York cyber rules may be harbinger

Effective March 2017, the New York State Department of Financial Services issued its "Cybersecurity Requirements for Banks, Insurance Companies, and Other Financial Services Companies."

The New York requirements may well be adopted as the model framework used across the country—and may also become a standard by which negligence is measured for non-compliance. These requirements set forth a variety of proactive cyber-security activities in which financial institutions must engage. Moreover, the regulations require that the board of directors or a "senior officer" certify that he or she has reviewed all of the relevant documents and that the institution complies with the regulations.

So, just as Ponemon remarks on the difficulty IT professionals have in educating their senior management on complex IT matters, the state of New York is requiring senior management to certify just such an education.

One saving grace may exist: "Senior officer" is defined as "the senior individual or individuals … responsible for the management, operations, security, information systems, compliance and/or risk of a Covered Entity…. ."

Thus, whoever at the financial institution is responsible for cyber security can be the senior officer who executes the certification, and not a member of the board or an executive officer.

The requirements state that financial institutions shall designate a chief information security officer (CISO). The CISO is responsible for implementing and overseeing the cyber security program and enforcing cyber security policy. This person can be either in-house or from a third-party service provider. The CISO is likely to be the senior officer signing off on the certification.

Why this is important to get right

Shareholders have filed several stock derivative lawsuits against companies whose directors and officers have experienced a data breach. These types of suits arise from allegations that ineffective or negligent corporate board oversight was a contributing factor behind subpar systems defenses and a breach that led to losses; a steep decline in share value; or both.

* Robert D. Chesler, a shareholder in Anderson Kill's Newark office, represents policyholders in a broad variety of coverage claims against their insurers and advises companies with respect to their insurance programs. Chesler is also a member of Anderson Kill's Cyber Insurance Recovery group. Mr. Chesler can be reached at rchesler@andersonkill.com or (973) 642-5864
Marc D. Schein, CIC, CLCS, a risk management consultant for Marsh & McLennan Agency, assists clients by customizing comprehensive commercial insurance programs that minimize or eliminate the burden of financial loss through cost-effective transfer of risk. Mr. Schein can be reached at marc.schein@marshmc.com or (516) 395-8504

Commentators expect that plaintiffs will continue to bring these suits until companies get it right. Compliance with a rule like the New York requirements may provide a strong defense for such claims. However, less than full compliance may provide a roadmap for future plaintiffs in such suits.

While the requirements are detailed and provide guidance, see, e.g., Sec. 500.03, uncertainty as to the exact parameters of the requirements will undoubtedly remain. Enforcement action and litigation may be necessary to clarify the duties of the company, its directors and officers, and the CISO.

D&O serves as main armor

So it's imperative that a company have the right insurance coverage to cover these emerging risks. Directors and officers liability (D&O) insurance policies are the main bulwark protecting directors and officers against shareholder suits. A company's best interests are served by making certain that D&O coverage is as broad as possible and does not contain any cyber exclusions.

In a case currently before the Ninth Circuit Court of Appeals, the policyholders' D&O policy contained a "breach of privacy" exclusion. (*Los Angeles Lakers vs. Federal Insurance Company*) Such an exclusion could limit coverage for shareholder suits arising from data breaches.

The New York requirements do not set forth any specific enforcement mechanisms. Instead, they simply state that "This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws."

Most likely the N.Y.S. Department of Financial Services will use its traditional tools of investigations, enforcement actions, and fines and penalties. These actions will lead to the same D&O coverage questions with which bankers are all too familiar: What is a claim? What is a loss? Are investigative costs covered? Are fines and penalties covered? Is defense cost covered?

A majority of mid- to large-cap financial institutions have by now purchased what is known as privacy and network security insurance or cyber insurance. These policies provide a variety of coverages, but at their core, they provide insurance coverage for the first-party legal responsibilities a company has post-breach and third-party damage arising out of data breaches.

Cyber policies often do not cover fines and penalties in the state of New York. Even privacy and network security policies may not provide coverage to the company for failing to comply with the requirements.

In this new interconnected cyber world, it is incumbent upon insurance professionals to educate their banking clients on the entire arsenal of potential cyber liabilities. However, a major issue facing the insurance industry is the lack of brokers who specialize in the ever-changing cyber marketplace.

We are seeing a large gap in insurance professionals who can competently advise and summarize a client's cyber risk profile; determine coverage gaps; and negotiate with insurance carriers to have the wording in policies read in favor of the client rather than the insurer.

Properly advising a client becomes incredibly difficult if brokers cannot comprehend the cyber exposure their clients face. This is why clients are strongly encouraged to work with a privacy and network security risk management expert who can quantify the cyber exposure, while being able to articulate the first-party legal responsibilities a business faces post breach, potential liabilities, and the nuances of a cyber insurance contract.

Evolution of cyber insurance

The first cyber policy was created nearly 20 years ago. The forms have consistently evolved, with the most dramatic changes occurring over the past five years. In 2017, more than 60 insurance carriers offer cyber policies. Unlike property and general liability policies that are drafted based from industry-wide standard forms, cyber insurance underwriters do not use standardized forms. This creates lack of consistency between insurance companies.

This makes the marketplace for this cyber protection product like the Wild West.

However, this also creates a potential buyer's advantage. Because many insurance companies are seeking to sell policies, banks can obtain maximum negotiation opportunity over price and terms.

* * * *

About Anderson Kill

Anderson Kill was founded in 1969 on the principles of integrity, excellence in the practice of law, and straightforward solutions to complex legal issues. The firm's attorneys approach engagements aggressively, and have earned a reputation for combining corporate polish with pugnacity. Based in New York City, the firm also has offices in Philadelphia, PA, Stamford, CT, Washington, DC, Newark, NJ and Los Angeles, CA, but the attorneys travel around the country and around the world to handle all types of matters. Anderson Kill attorneys work together, leveraging creativity and legal and business acumen to deliver cost-effective resolutions to clients' problems. Many of the firm's professionals are recognized experts in their practice areas, leaders and active participants in professional associations, and are frequently invited to speak to business organizations.

Anderson Kill clients include some of the nation's largest public and private entities, including companies in financial services, retail, oil/gas, telecommunications, construction, food supply, technology, pharmaceutical and life sciences, and utilities, municipalities and state governments, religious and not-for-profit organizations, small companies and individuals. Anderson Kill prides itself on attracting and retaining intelligent, personable and well-rounded attorneys. Smart attorneys with sharp skills, excellent client service, and a track record to prove it: that is the Anderson Kill difference.