CLM CLAIMS & LITIGATION MANAGEMENT ALLIANCE™

ADVANCING ETHICS, COOPERATION AND EDUCATION

CLM 2015 Cyber Liability Summit
October 21, 2015 in New York City

# Be Prepared or Face the Consequences

## I. Making Sure "Your is House is Clean" - Strategic Approach to Cybersecurity

A business should have a strategic approach to cybersecurity, which includes performing a risk assessment of its current computer network, as well as policies and procedures. A risk assessment helps to identify vulnerabilities, either internally or externally, that may pose a threat. Additionally, a risk assessment will help a business understand how well-equipped it is to protect against, detect, and respond to cyber threats. This will include a full range of internal and external assessments to evaluate its systems, applications, and facilities, including: cyber risk assessment and analysis; vulnerability assessment and penetration testing; physical security assessments; breach and compromise assessments; and wireless security assessments. A proper risk assessment should also include a review of a business' current policies and procedures to determine if same are appropriate, enforceable, and effective.

Similarly, a business must perform a "Standards-Based Assessment" to determine what laws, regulations, standards, etc. apply to them. For example, pursuant to the National Institute of Standards and Technology ("NIST") log files should be backed up and archived regularly. See Natl. Inst. Stand. Technol. Spec. Publ. 800-123, 53 pages (Jul. 2008). The retention period for archived log files depends on a number of factors, including the following: legal and regulatory requirements, organizational requirements; size of logs (which is directly related to the traffic of the site and the number of details logged); and value of server data and services; and threat level. (Ibid.) Another example is the Payment Card Industry Data Security Standard ("PCI DSS"), which applies to the securing cardholders' information that businesses store, process, and transmit.

Lastly, a proper risk assessment includes reviewing a business' current plan for responding to a data breach in a timely manner. This includes a variety of specific elements and covers a wide-range of disciplines. A proper rapid response team is generally comprised of strong, capable representatives who will ensure an efficient executed response. The "Incident Lead" is normally outside counsel who will serve as the "captain" of the team, and, among other things, ensure that the attorney-client privilege is maintained. Other members of the team include executive leaders, IT department, in-house counsel, forensics, public relations, customer care and human resources, and an insurance broker.

## II. Creating and Developing Policies and Procedures

Once a risk assessment has been completed, a business should create and develop information technology standards, policies, and procedures that are appropriate, enforceable, and effective within applicable laws and regulations. This includes creating a cyber committee to develop and implement a risk management plan for preventing a data breach. Once a committee has been established, this committee will draft policies regarding the privacy and security of business data, which includes the use of encryption, remote access, mobile devices, laptops, email accounts, and social networking sites. In addition, the committee will develop data classification. This includes performing an inventory of the software systems and data, and assign ownership and categorization of risk; the higher the sensitivity of the information, the stronger the security protections and access control must be.

Being proactive is crucial to preventing a cyber-attack. Thus, a business through either its own IT department or the retention of a third-party consultant should conduct periodic vulnerability scans, penetration tests, and malware scans to protect against potential data breaches, as well as to identify new vulnerabilities. Additionally, regularly training employees as to these policies and procedures is vital. Employees must be aware of a business' security protocol in place, and be taught how to prevent accidentally exposing a client's personal, confidential information.

Lastly, as part of creating and developing policies and procedures a business should review third party vendor contracts to ensure it is protected not only from a breach within the company, but one caused to a third-party handling your customers' personal identifying information. This should include analyzing these agreements for indemnity clauses, limitations on liability, insurance requirements, and, overall, guidance on which party will be expected to pay in the event of breach.

## III. Practicing Rapid Response Plan

Once a policy and procedure is in place, a business should consider testing its readiness to respond to a real attack and implement same. A good way to do this is by performing Table-Top exercises, which simulate a cyber-attack and incident response. This will not only to prevent future attacks, but help a business to be ready in the event one occurs in order to maintain business continuity.

## IV. Insurance Considerations

Due to potential for significant damages and loss of reputation, a business should examine all insurance policies to ensure that any policy in place covers the type of loss associated with a cyber-breach. For example, an Errors & Omissions policy covers liability for economic damages resulting from a failure of defined services, and may contain exclusions for data and privacy breaches. A Property policy normally covers tangible property, which does not include data. Thus, a business should consider purchasing a Cyber Liability policy to cover such a claim. This includes retaining an insurance broker well-versed in cyber coverage in order to procure the right policy.

Some businesses are starting to think outside of the box in obtaining cyber insurance. When insurers balked at the prospect of covering the University of California's cyber risks because of

the vast scope of potential liability exposures associated with higher education and health care, Chief Risk Officer Grace Crickette asked them do something they had never done before suggesting the underwriters try "reverse-underwriting," a process similar to reverse-engineering, in which something is taken apart to see how it works in order to duplicate or enhance it. If the university met all the cyber security protocols set by underwriters, then the policy would respond to any losses that might occur. If not, the university would be left to fend for itself. The end result was a $5 million cyber liability policy responding to all damages and expenses stemming from a university data breach, including notification costs, forensic investigation expenses, credit monitoring, identity restoration and call center services.

## V. New Legislation

The House of Representatives recently passed a bipartisan cybersecurity bill to make it easier for companies to share cyber-threat information with the government and thwart hacks by criminals, terrorists, and rogue nations.

In the first action taken by the new Congress in response to recent high-profile cyber-attacks, lawmakers voted 307-116 to approve the Protecting Cyber Networks Act, which was previously passed by the House's Permanent Select Committee on Intelligence. The Senate intelligence committee passed its own cybersecurity information-sharing bill in March of this year, which they hoped to bring it to the floor shortly. Both the House-passed bill and the bill approved by the Senate intelligence committee offer liability protection to companies to shield them from lawsuits that could arise from the sharing of business records with the government and with one another. Previously, businesses have been reluctant to report to the government a cyber-attack out of fear of lawsuits from consumers or privacy groups. However, the proposed bill would shield businesses from liability and encourage the sharing of information. One key difference between the two bills is that the Senate bill requires any information shared by private companies to first go through the Department of Homeland Security, whereas, the House bill would allow companies to share their cyber-threat information with any civilian agency. Thus, for example, a bank could go straight to the Treasury Department for assistance related to a cyber-attack.

The bill passed by the House also makes the federal government liable for violations of privacy and civil liberties, and allows citizens who believe their privacy has been violated to seek damages from the government in Court.

Recently breached companies such as JPMorgan Chase, health insurer, Anthem, aviation companies and automobile manufacturers are actively lobbying and supportive of the cybersecurity information-sharing bills with the hope of limiting their liability.

Despite these new laws, there are many who believe that it will not significantly reduce security breaches, and that the private sector is already doing a good job of information sharing. Moreover, critics do not believe the information sharing bill addresses the real problem that sophisticated hackers will continue to penetrate what are in many cases inherently vulnerable systems.