2016 CLM Annual Conference
April 6-8, 2016
Orlando, FL

The Experts Speak – Cyber and Data Privacy Risk

I. Placing and Providing the Right Insurance for the Need

Understanding the Insured's Exposures, Risk of Loss and Compliance Requirements

Placing and providing the right coverage requires an understanding of the nature of insured's business and where the risk lies. While brokers work with an insured to understand the needs and recommend the best coverage, the underwriters need to understand the risks facing the insureds to ensure that they are providing sustainable insurance products. Some of the same questions answered by brokers drive the underwriting.

Of significance is knowing the business. Is the insured a large health care provider with a national footprint, or a local physician with a client base of 20 square miles? How are payments made and what data is kept in house? What access do employees have to sensitive data? How are client communications made and in what form? Does the insured utilize vendors who have access to sensitive data and what agreements are in place? Has the insured undergone a risk assessment and do they have an incident response plan or even a Written Information Security Plan? What technology do they have and how is it maintained?

Critical is knowing the biggest loss the organization will face in the event of a Data Privacy event. For some organizations, even short-term disruption to email capability is devastating to their operations, for others it's the possible loss of intellectual property, and for some it's reputational. These questions need to be answered to understand the insurance needs and the insurance risk.

Identifying and Classify the Data

In addition to understanding the insured's business for risk evaluation and product selection, it is vital to identify the data collected and maintained by the insured. For instance, if the insured is a local physician utilizing paper records and paper billing submissions, the data privacy needs are more limited than a national urgent care center

maintaining nationally accessible online patient records, accepting credit card payments and submitting health insurance reimbursements online. While that may be a simple comparison, it illustrates the need to evaluate the risk on a one on one basis for each prospective insured.

Other important details of the data include, where and how it is stored and for how long. What employee training has occurred regarding access to and maintenance of the data helps to understand the risk of a breach due to employee inadvertence or negligence vs. a mere risk of third-party activity.

Challenges

Cyber security and data privacy risks are complicated and costly. Proper treatment of these risks requires a layered approach and a combination of risk management techniques including risk avoidance, contractual transfer, risk retention, risk control and risk transfer.

However, not all cyber security of data privacy related exposures can be avoided, prevented, or contractually transferred – it's just the nature of the beast. The financial losses including data response costs, forensic costs, loss of income, loss of digital assets, damage to critical infrastructure, civil law suits, regulatory actions, state and/or federal fines/penalties, extortion monies, credit monitoring, credit/identity restoration services can be enormous but these are insurable risks. The uninsurable risks of reputation damage, loss of brand equity, and societal harm are challenging to measure, which makes it difficult to control.

Cyber-attacks and data breaches are likely to be the rule rather than the exception for businesses of all types going forward, which is the focus of many discussions the boardroom these days. Identifying cyber and privacy risks as enterprise-wide risk management concerns and implementing preemptive risk mitigation controls and measures is just fundamental and the boardroom plays a critical role in this effort.

Board of directors have a fiduciary duty to protect the organizations assets and interest on behalf of shareholders. Failure to address cyber and privacy risks in the boardroom could give rise to consumer class-action suits and shareholder derivative suits alleging directors did not met their duty of care and/or duty of loyalty to the organization.

Board risk oversight, at minimum should include:

1. Adopting an organizational culture of privacy and security vigilance;
2. Ensuring that regular privacy and security risk assessments are being performed;
3. All employees from the top down are adequately trained;
4. Comprehensive privacy and data security policies are in force;
5. A tested and practices incident response plan of action is in place.

Market Conditions – A Brokers View

A hardening cyber insurance market persists, particularly for health care and retail risks. Premiums are higher, capacity is somewhat restricted and underwriting scrutiny is heightened. The driving force is, of course, losses: in the past 18 months, major claim have hit not just primary underwriters, but excess underwriters through layered towers of $100M to $150M in limits.

The cyber market is not expected to flatten out any time soon. Further, cyber threats, are escalating, with concern with U.S. infrastructure and businesses could be under attack from cyber criminals with varying agendas. Growing technology risks associated with the expansion of the mobile workforce, broad adoption of "bring your own device" (BYOD) policies, and innovations, such as wearable technologies and the internet of things (IoT) will only expand threats to data privacy and security.

II. Underwriting Loops: Actuaries and Claims the Great Big Circle of Information

Underwriting Drives the Products Offered

In conjunction with actuaries, underwriters perform a thorough analysis of the cyber landscape in order to help shape the insurance company's strategy in terms of industry focus. The underwriting approach will include, areas that they will not underwrite, whether the segment of business upon which they focus will be large corporate risk, middle market or small commercial. The approach to underwriting will differ based on the target market. As the landscape evolves, underwriting approaches need to keep step in order to remain competitive and viable in the market.

A large portion of data upon which underwriters rely is claims data. Claims data includes types of claims made, claim expenses, length of claim lives, proactive offerings, and the actual offset of proactive undertakings to claim volume. It is vital to an insurance company's ability to provide adequate insurance products and that the underwriters work with claims and actuaries to understand and develop the company's insurance portfolio.

The Great Big Circle of Information shared between actuaries, underwriting and claims results in not only the initial target markets and insurance product offerings, but also re-analysis of insureds at renewal time, application amendments, application tailoring to understand new founded risks and repricing. These are important to ensure that expectations of all are met when a critical event arises.

Benefits of Claims Information on Underwriting

Regular roundtables between claims and underwriting enlightens all on the evolving law, emerging trends and their respective impact on the existing cyber insurance product line. An internal claims team is the best suited to relay the rapid evolution of

Data Privacy trends, risks and impact to underwriting and such communication can result in mid-stream policy changes. Certain types of policies are amenable to policy changes and amendments to better position the broader insurance book while at the same time fulfilling the expectations of all involved. For instance, some insurance policies may not have been originally designed to cover a Data Privacy Event, but ultimately did in fact provide such coverage. In recent year, coverage for Data Privacy Events (though not intended originally) have been found in general liability policies, directors and officers policies and professional liability policies. Conversely, some cyber policies were drafted in a way which could arguable excluded coverage for certain intended events. Policies changes may be appropriate also where exposures have changed and additional more specific, or broader coverages become available.

Underwriting the Future

Today, the changing threat environment coupled with the ever-changing legal and regulatory landscape, creates a reality that companies of all sizes cannot afford the risk of being unprepared for a data breach and as such, essential preparedness should include either risk mitigation or risk transference. Emerging threats are no longer simply emanating from a disgruntled employee looking to publish coworkers' personal information on social media or a cyber-extortionist looking for $50,000 to unlock your network. Instead, attacks are stemming from different constituents ranging from malicious targeted attacks and foreign espionage to supply chain disruption and careless staff. Additionally, regulators have become increasingly aggressive in leveraging fines and penalties for non-compliance.

Accordingly, today's cyber security insurance responds to these risks. In general, the policies provide both first-party and third-party risks. First-party coverage may include business income/extra expense coverage, Data Asset Protection, Cyber Extortion and most importantly, Crisis or "Event" Response. Policies may be tailored to include any or all of these coverages but nearly all contain Event Response coverage. Specifically, business income/extra expense coverage will provide for loss of business income resulting from a data breach. This coverage may also extend to provide coverage for dependent business interruption if caused by a critical vendor. Data Asset Protection is also afforded and typically includes the cost of repairing and restoring computer systems and intangible assets that are corrupted or destroyed by a computer attack. Cyber-Extortion coverage provides for costs of consultants and extortion monies for threats related to interrupting systems and releasing private information typically targeted by Ransomware requiring payment to unlock the compromised network. Finally, the most important first party coverage is Event Management or sometimes called "Crisis Management". Encompassed within this coverage are the following costs resulting from a security incident: Forensic Investigation Services, Breach notification services (including legal fees and call center services), Identity monitoring expenses as well as the cost to retain a public relations firm.

Third party coverages typically include Privacy Liability, Privacy Regulatory Defense Costs, and Network Security Liability. Privacy Liability provides for the

defense and liability for failure to prevent unauthorized access, disclosure or collection of confidential information or third party corporate confidential information, or for failure of others to whom you have entrusted such information (e.g., data storage facility, credit card processor or other critical vendor). This coverage also extends to include liability for failing to properly notify of a privacy breach and claims are typically brought by customers, employees and trading partners. Privacy Regulatory Defense Costs include costs to defend an action or investigation by a regulator due to a privacy breach, including indemnification for any fines and penalties assessed. Finally, Network Security Liability provides defense costs and liability coverage for failure of system security to prevent or mitigate against a computer attack including but not limited to spread of a virus or a denial of service. Failure of system security includes failure of written policies and procedures addressing technology use and these claims are typically brought by third parties, customers and employees.

In addition, policies have expanded to provide coverage for PCI fines and penalties if assessed in a jurisdiction where insurable.

Most recently we have seen incidents that may have been perpetrated by a Cyber attack but result in actual physical harm such as bodily injury and/or property damage. Three relevant examples include the Stuxnet attack in 2007, the German Steel Mill explosion in the latter part of 2014 and most recently, the coordinated attack on the Ukrainian Power Grid. In these cases, it is not simply hackers looking to gain access to your personal information but even more catastrophic, causing actual tangible harm. At present, Cyber Liability policies do not contemplate these exposures. As such, it is important to look to your CGL policy for coverage.

As cyber and technology risks continue to evolve, cyber insurance coverage will as well. Insurance companies are continuing to accumulate more actuarial data, based on the loss history of various industries, each corporate customer's use of technology and the corporation's own level of security.

III. Claims, Breach and Litigation

Generally, the first question asked by claims when notice of a claim is made is – is there coverage? There are no reported decisions concerning coverage on standalone cyber policies. One bad decision could turn the industry on its head. Consistency is critical to the industry as a whole. Other coverages may also be available and should be evaluated (E&O, D&O, CGL, property and crime policies all may be a source of additional coverage).

The breach response team is assembled, including counsel. Since the perspective here is mitigating the risk – it should be noted that the risk is two-fold. First, the risk is non-compliance with various breach notification laws and federal statutes. Second, the risk is subsequent litigation. Breach counsel and claims are aligned in this regard with the insured's interest of risk mitigation.

The Risk Starts before the Breach

The US Department of Justice Cybersecurity Unit, Computer Crime & Intellectual Property Section of the Criminal Division published "Best Practices for Victim Response and Reporting of Cyber Incidents." The Best Practices also reference the National Institute of Standards and Technology (NIST) framework published in 2014. Businesses and organizations routinely underestimate their responsibilities and expectations with respect to safeguarding personal information and often when a breach occurs the damage is largely done.

The Best Practices document was specifically drafted to assist organizations in preparing a cyber incident response plan and to prepare for cyber incidents. The valuable collaboration between federal prosecutors handling cyber investigations and private sector companies that have managed cyber incidents resulted in a well set out framework for smaller, less well-resourced organizations to follow. The first step for any organization that houses any personal information should be to read and implement the best practices set forth in the document. As stated therein, well established plans and procedures in place for managing and responding to a Data Privacy event is a critical first step for the ensuing event.

Reflecting back upon the first section Understanding the Insured's Risk is also a good indicator of where to start in establishing the plan and procedures for managing and responding to these events. The aspects of the business operations which are most critical to the business/organizations continued operations should be the priority as it is both the most vulnerable and the most important. The action plan should delegate responsibility for handling certain tasks during an event. The time lost in creating this on the fly can make the difference in minimizing the damage.

Response is still Critical

We have been talking about breach response so much that it may be taken for granted. It does however remain one of the most critical steps in mitigating the event. The first immediate step is to concretely (if possible) identify the nature and scope of the incident. Is this malicious or a technological mishap? Computer logs will be vital to this process and will aid in determining the number of affected systems, origin of the incident, malware used in connection with the incident, remove servers which exfiltrated data and possibly the identify of victims. Concurrently, steps should be taken to minimize continuing damage. For instance, shutting down the network, rerouting network traffic, blocking a denial of service attack, and isolating the affected parts of the network. Proper preparation would mean a back-up copy of the network exists and can be utilized to maintain organizational business.

An image of the affected computers should be made which preserves a record of the system at the time of the incident for analysis and possibly for use in future litigation. Also evidence needs to be preserved so that the organization can properly trace back its steps and the root cause if subsequent litigation ensues.

Most often small to mid-size businesses are overwhelmed by the notion that they must provide specific written notification to all affected persons (persons who had personally identifiable information accessed). At least 47 states in the United States have database breach notification laws requiring organizations to notify affected persons. Each state law is different: some prohibit notification where law enforcement is still investigating, and some allow a pass on notification if after consultation with law enforcement there is a conclusion that there is no reasonable likelihood of ensuing harm. Also, many states require notice to the state's attorney general office or other law enforcement entities.

Protecting the Evidence

Attorney-client privilege and attorney work product remains one of the best shields to an organization to its obligation to produce potentially damaging information during a subsequent litigation. *Upjohn Co. v. United States*, 449 U.S. 383 (1981) ("The attorney-client privilege is the oldest of the privileges for confidential communications known to the common law."). Also, Federal Rule of Civil Procedure 26(b)(3) protects work product from discovery. "Ordinarily, a party may not discover documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent)."

With outside counsel, the attorney-client privilege analysis is simply whether the communication between the client and attorney was confidential and for the purpose of obtaining legal advice. *See, e.g.*, *United States v. Chen*, 99 F.3d 1495, 1501 (9th Cir. 1996), *cert. denied*, 520 U.S. 1167 (1997). In cyber specifically, a major decision in *Genesco, Inc. v. Visa* protected the cybersecurity consultants' work product and communications. The *Genesco* Court held that—like that of other retained experts—forensic consultants are subject to confidentiality under the attorney-client privilege and/or the work product doctrine when counsel retains the consultants for the purpose of obtaining technical assistance to enable counsel to render legal advice to a client. Absent the role of outside counsel in the breach response, the work product of the forensic team would be discoverable. Putting in place the breach response team as a whole, allowed the victim in *Genesco* to obtain data about prior Data Privacy events, the instant Data Privacy event, make the necessary modifications and correct the problem without the threat of educating the Plaintiff in the subsequent litigation.