

CLM 2016 Cyber Liability Summit
October 5, 2016 in New York City

The Future of the Cyber Claims Adjuster: A Jack of All Trades

I. Cyber Risks Are Expanding as Businesses Incorporate Technology

Understanding The Risks

Businesses are incorporating technology into their plans to maximize profitability. As a result, new risks are emerging and traditional risks are being recast in a different light. As underwriters work with insureds to manage their risks, the cyber insurance policy is evolving to address these concerns and mitigate exposures. The cyber claims adjuster's role will transform beyond data breach and expand into new technology based claims, including those traditionally reserved for other insurance policies, such as property and bodily injury. To effectively manage these risks cyber claims adjusters will need to develop knowledge in multiple disciplines and become a "Jack of All Trades".

Traditional Risks

Although the cyber industry is relatively young and is still in its infancy, the exponential and prospective growth has transformed cyber into becoming a market leader. Cyber has focused on data breach response and vendor management of those risks. While these risks remain at the forefront of the industry, as the cyber market matures, insureds are interested in more than traditional risks in an effort to take advantage of the technological revolution that is taking place and are looking for insurers to protect their interests and the interests of their shareholders from catastrophic losses.

What are the Emerging Risks?

The maturity of the cyber market has caused insureds to re-evaluate their business plan and re-examine the most effective manner of managing their emerging risks – business interruption, internet of things (IoT), intellectual property, privacy, security liability, technology errors & omissions, and data restoration.

Insureds have identified a myriad of different potential attackers in the industry, including plaintiffs' counsel, regulatory agencies, nation-states, business competitors, employees and consumers of their products/services. Any of these potential attackers could create a risk that results in significant exposure to the insured. Insurers are attempting to address these potential actors and the claims they may submit by expanding the scope of a cyber insurance policy to meet the needs to the insured and mitigate the insured's technological exposures.

II. The Emerging Risks

Business Interruption

Business interruption is not just a consequence of property damage – it is anything that interrupts a business, including cyber attacks that trigger a non-physical business interruption event. As businesses realize that they are increasingly relying upon technology for their operations, they are looking to insurance policies for coverage in the event their business is interrupted and suffers a loss.

Attackers are constantly looking for new vulnerabilities to exploit. It is well known that cyber extortion is a thriving industry, as businesses pay ransoms for the key to unlock their servers. The growth of this criminal industry is strongly based upon the potential business interruption associated with the business being locked out of its critical data. How can a business function without access to vital information regarding its goods and services? A physician is significantly handicapped if unable to access historical patient data when rendering medical services to a patient. A shipping company is unable to address logistics with vendors if unable to access information detailing the status of its various shipments.

The inability to access data vital to business functionality, whether from a hacking of the IT system, the negligent acts of an employee causing a software/hardware failure or some other cause, the exposures can quickly be significant and may potentially exceed policy limits. Timely consultation with the insured and management is essential to mitigate the losses associated with such an exposure.

IoT

IoT, the Internet of Things, has become an acronym synonymous with growth in the cyber industry. Gartner, Inc. forecasts that there will be 6.4 billion connected "Things" in use in 2016, up 30 percent from 2015, and that by 2020, there will be 20.8 billion connected "Things". This type of exponential growth considers the mass marketing of autonomous automobiles, connected homes and businesses, wearables, automated production, smart cities and numerous other goods/services. As development of these cyber products increases, the correlating risks and exposures associated with the cyber market with similarly increase.

But the management of these risks may not fit the traditional role of the cyber claims adjuster. The typical cyber policy does not cover an automobile bodily injury claim caused by a technology failure in an autonomous motor vehicle. Similarly, what happens when a hacker infiltrates a business' servers and turns off all of the fans in their computers, causing the equipment to overheat and start a fire that results in bodily injury, property damage and business interruption?

Although these risks are not traditionally covered under a cyber policy, insureds will certainly be seeking coverage for these types of risks in an effort to manage their business. The cyber claims adjuster's role will likely evolve to include these traditional risks and exposures.

Intellectual Property

The "crown jewel" of any business is its intellectual property – trade secrets. Whether it is the secret formula for WD-40, the secret sauce recipe for the Big Mac, KFC's recipe for coating chicken with herbs and spices or Coca-Cola's secret formula, corporations are protective over their market advantages. Should trade secrets be maintained on a business' servers, it becomes a cyber exposure. Typical insurance policies have not afforded coverage for trade secrets. As a result, a business may find that its' most important asset has no protection other than what the IT Department has installed to protect against intrusions.

Faced with this unmitigated risk, businesses may choose to remove the trade secret from its' servers and revert to more traditional methods of securing the intellectual property, such as writing the trade secret on a piece of paper and locking it in a vault. But such Draconian tactics may not permit the business to efficiently function to maximize profits. Consequently, insurers may be called upon to provide coverage for these types of claims as businesses strive to maximize technological developments.

Industry concerns surrounding the coverage of intellectual property range from the valuation of the intellectual property to the insured's willingness to disclose safeguards implemented to prevent others from improperly accessing their trade secrets. As competition in the cyber industry increases, insurers may find themselves increasing the scope of coverage for this risk and the cyber adjuster must be equipped with the knowledge of how to handle these claims.

Privacy Liability

Plaintiffs' counsel and regulatory agencies, such as the FTC, have strongly advocated for privacy rights and damages associated with a business' failure to keep information private or for failure of others, such as a credit card processor, that have been entrusted with information to keep it private. The failure to maintain the confidential proprietary information from the public may result in litigation by customers and employees or a regulatory action.

Privacy liability is not limited to the failure to maintain information private; rather, it is inclusive of a business failing to properly notify an individual of a privacy breach. As such, claims adjusters should have a comprehensive perspective of privacy liability.

It is imperative that a claims adjuster understand and be up to date on the evolving exposures associated with privacy liability and efforts being made by the plaintiffs' bar to expand exposure for these claims.

III. Other Insurance

The growth of cyber insurance into new spaces will assuredly lead to situations in which multiple policies respond to the same claim. It is critical that early in the claims process the adjuster work with the insured to identify all policies that may cover the claim, including any third party policies that may provide coverage to the insured, and conduct an analysis of the policies' other insurance clauses. The early assessment of the claim will allow the claims adjuster to know whether they are primary or excess on the claim and whether the quantum of the loss may impact the insurer's and reinsurers' layer.