CHECKLIGHT®
BY SERA-BRYNN

Insurance Against Cyber-Crime: Trying to Form a Common Front

The crooks are evolving and getting smarter.

Agents, underwriters, and IT experts are scrambling to make sense of the current cyber risk management environment, but they're speaking different languages and struggling to create an effective message.

Meanwhile, insureds …yes…that includes agencies such as yourself…try to guard their tech infrastructures but too often fail on basic defensive measures like software patches and penetration testing.

Welcome to the state of the cyber insurance market in 2021. Observers from industry sectors are sorting out the trends and options, while seeking an approach that meshes their respective strengths against sophisticated, well-capitalized criminal groups.

Agents in the trenches are seeing trends meant to limit exposure and at the same time fortify client defenses in multiple ways. Some key observations:

- Carriers are trying to streamline the underwriting process, which often involves creating exclusions that tighten the range of coverage afforded
- Prospective insureds now need to demonstrate hardened network security and loss control technology
- Government and industry-specific cybersecurity compliance standards, and the acronyms that are associated with them like NIST SP 800-171 and DFARS 252.204-7012 are emerging as threshold barriers to entry for terms and conditions that effect meaningful coverage

Underwriters have good reason to be cautious about their pricing and loss control expectations, given the market smarts exhibited by hackers. Like the COVID-19 virus, the threats are constantly mutating. Criminals know all about insurance and its impact on companies when they respond to losses. From their research, criminals increasingly assess what companies have insurance and how that plays a role in their selection of targets. Extortion, such as the payment demands linked to ransomware, reflect carefully considered financial analysis; they understand financial capacity, who has insurance, and where to apply pressure. There's nothing random about it.

Sophisticated hacker gangs will penetrate a target's network and spend months deciding how to capture sensitive data while also analyzing gross revenues, net profits, insurance coverage, strategic plans and other factors to build into a ransom demand. Think criminal MBA case studies with collaborators drilling down into corporate governance, financials, and operational pressure points to formulate an "offer you can't refuse". Quite literally. This is vastly more alarming than attacks by unscrupulous internet vandals. Hackers and their state sponsors are mounting all-out digital warfare on vital infrastructure.

Against such patient and skilled attackers, cyber insurers are facing increasingly frequent and more severe losses. Faced with enormous claims, they are responding in a predictable fashion: less coverage, more exclusions and higher premium…as in multiple double-digit increases.

Agents are urging clients to effectively respond to these trends by getting smarter on the basics of security.

- Employers must be insistent on **training and culture** to help their staff navigate phishing, social engineering, and other dubious appeals intended to roll the digital Trojan Horse past the corporate watchtowers. Strict precautions help prevent attacks; a lax attitude can create big headaches and are symptomatic of an otherwise preventable moral hazard that can result in severe consequences.

- IT system maintenance is a condition paramount. Cyber insurance coverage assumes that insureds will keep their **network and software up to date and patched**. "Failure to maintain" is a primary basis for claim denial. System updates are not upselling…they are a tech companies' response to documented vulnerabilities that criminals are ready to exploit. Failing to maintain a network with current software is the

most egregious and avoidable form of moral hazard in cyber insurance. Indeed, it is at the root of many disappointing loss adjustment outcomes. Like poor employee awareness, system hygiene is a consequence of disengaged management, and an absence of diligence.

This issue is especially acute for small businesses that lack dedicated in-house IT departments savvy in security matters. Since they often rely on third parties to maintain these systems, cybersecurity is out of sight and out of mind. (…and keeping a business afloat during a pandemic has done nothing to help this reality). Everything is fine until the hackers hit and managers are bushwhacked by ransom demands or disruptions that they never saw coming, because they weren't looking.

- An emerging, highly effective, and increasingly available part of the defensive strategy now includes a robust **continuous network monitoring and log data management** service to identify threats and notify administrators of breaches and anomalous behavior *as soon as it occurs*. Such a capability allows company executives and their IT teams to identify the point of entry and malicious code, and qualify severity of breaches faster, which leads to an accelerated quarantine and more focused response. Log data complements forensic analysis with more exacting evidence, which shortens recovery, and materially changes severity.

The need to change extends to insurers, agents, IT departments and security providers. They are learning to speak one another's languages to demolish functional silos and integrate their capabilities. That collaboration is essential because cyber insurance is hindered by the asymmetry of knowledge among the parties:

- Insurance producers rarely have a command of the language, methods or culture shared among IT professionals.
- IT professionals rarely allow for the caution (seen through limitations and exclusions) that carriers build into their policies as a matter of essential insurance practice and self-preservation.
- Businesspeople often relegate cybersecurity decisions to non-executive talent out of denial and ignorance. The reality is that cyber exposure now possesses non-delegable severity which executive management must now own.

As discussions among stake holders in the cyber security dilemma unfold, underwriters are already incorporating technology into their risk selection. Insurers are turning to tech firms, for example, to assess an insureds' network security measures. These assessments vary in their usefulness, ranging from non-invasive network "scans" that combine the curb appeal of a report with a low efficacy risk avoidance activity, all the way up to SIEM (Security Information and Event Management) relationships that provide expensive but reliable continuous monitoring and dedicated IT talent for larger, better capitalized insureds.

A representative midpoint approach between these low and higher cost options involves emerging EDR technology (Endpoint Detection and Response) paired with CLM (Centralized Log Management). These services provide scalable, affordable, and highly effective risk avoidance capabilities to insureds. *A product like CHECKLIGHT is representative of such a solution and is backed by a $250,000 performance warranty. The product is currently an endorsed solution of IIAV.*

EDR tools bolster defenses using data analytics and machine learning which can sift through enormous amounts of datapoints to find patterns and anomalies able to flag potential threats and actual breaches before they can do substantial damage. Indeed, underwriting managers are incorporating these tools into how they build out their insurance offering for potential clients.

Cybercrime is a fundamental threat to our economic infrastructure and national security. While most primary forms of insurance result from methodologies well over a century old, the emergence of cyber as a universal exposure has arisen within a couple of election cycles. Impacts from network incursions have placed enormous urgency and stress on businesses, the people that lead and are employed by them, and the institutions that serve and protect them. Beyond insurers, agents and security providers, state and industry regulators are taking action to frame cyber management financial responsibility and create enforceable policies that can offer guidance and shape expectations. Some regulatory bodies are now adding teeth to their policy guidelines with concrete standards and financial penalties for non-compliance. Initiatives include:

- New York: DFS Cyber Security Regulation (23 NYCRR 500)
- California: Consumer Privacy Act (CCPA-CA AB 375)
- ***Virginia: Insurance Data Security Act***

- Securities and Exchange Commission's refinements to policies regarding incident response
- Department of Defense's implementation of DFARS 252.204.7012
- U.S. Department of Health and Human Services HIPPA Security Rule
- ***NAIC-Insurance Data Security Model Law***

Standards organizations are also taking steps to bolster compliance efforts:

- NIST Cybersecurity Framework
- ISO 27001 – Information Security Management Systems
- Center for Internet Security (CIS) Benchmarks

The sheer pervasiveness and severity of cybercrime makes the insurance treatment of it essential to the workings of modern society. Attacks now infect everything: businesses, financial systems, schools, hospitals, and water and electrical utilities. Nothing is off limits.

Insurance can help hedge losses from cybercrime, but it will need a strong complement of prudent and realistic risk avoidance, loss control, and inspired underwriting. Taken together, insurers and their insureds will have a fairer chance financing a threat unlikely to ever vanish, with hopefully diminished catastrophic potential, if they view the problem through an interdisciplinary risk management lense.

To learn more about IIAV endorsed CHECKLIGHT continuous network monitoring, contact Charlie Hoover at 919-522-2164 or Don Bragg at IIAV.