RE-ISAC Weekly Cybersecurity Report

Real Estate ISAC Information Sharing and Analysis Center

*Serving the Commercial Facilities Sector*

**20 September 2017**

**TLP GREEN**: Limited disclosure, restricted to the community. Sources may use **TLP GREEN** when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share **TLP GREEN** information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP GREEN** information may not be released outside of the community.

## INTRODUCTION TO CYBER INSURANCE

**IN BRIEF**: Businesses of all sizes have an ally in mitigating risk related to cyber incidents. Cyber insurance policies have been in place for several years, now. That said, we must remember that the purpose of insurance in general is to prevent a major financial loss. Hopefully, adequate cyber insurance can help prevent small and mid-sized businesses from closing their doors in the wake of a cyber incident. This offering is still in its early growth stages, and the industry is still studying the problem. As a result, policies can vary greatly and it is common to have a policy that provides inappropriate or inadequate coverage for an individual organization. It is crucial that an organization understand its own risk picture and obtains a policy tailored for its unique situation. It is also critical for firms to understand what policies do and do not cover and under what circumstances.

**KEY TAKEAWAYS & RECOMMENDATIONS**:

- Cyber insurance does not replace an effective cyber security program.
- Cyber insurance excludes coverage under some circumstances.
- Cyber insurance is still new and the legal and regulatory frameworks, as well as understanding of the risk and resulting impacts, continue to evolve.

**BACKGROUND**. Just as cyber risk and risk appetite differs for each organization, cyber insurance policies have many variations as well. As of 2014, just under one third of US businesses had any form of cyber insurance coverage. Within highly regulated sectors, approximately 50% of businesses had some form of coverage. The low rate of adoption partially stems from many myths and misconceptions. Some of them are:

- **Not Us**. We are not really at risk, we are not likely to suffer a data breach, we don't have anything an adversary would want, we are too small to face a cyberattack. – *Statistically speaking, more claims are filed by small businesses than any other size businesses*. Furthermore, recent events have demonstrated that cyber events can happen to anyone and may not always be targeted. Organizations should conduct a thorough risk assessment that considers the current threat landscape. A prioritized list of assets and risks can help organizations select the best types and amounts of coverage.
- **Resource Priorities**. We would be better off spending our money on preventative measures rather than paying insurance premiums. - Even if it were possible to completely prevent a cyber incident, an organization could be affected by a third-party or experience accidental - as opposed to malicious - cyber incidents. Furthermore, unless incident management, response costs, and liability damages are built into the budget (and sometimes, even if they are), the organization will need insurance coverage. The better question in this case is can businesses afford ***not*** to obtain coverage?
- **Doesn't Work**. Insurance providers don't pay claims or the coverage is not enough to make a difference in a major incident. – Sadly, there have been several high-profile cases where companies have sued their insurance provider

over disputes of unpaid claims. There have also been several high-profile privacy breaches where insurance providers paid on claims, but coverage fell woefully short of the costs actually incurred. These problems can both be avoided. Business seeking coverage must conduct a thorough risk assessment and obtain realistic impact projections on potential costs and losses as well as the likely hood for all possible cyber risks. Insurers must base rate calculation formulas on relevant factors that affect likelihood and impact of cyber events. Unfortunately, neither those selling insurance policies, nor the buyers of insurance within an organization, are cyber risk experts. Last, the state of the industry is that many policies remain highly negotiable and customizable to fit each organization's risk picture appropriately**. A thorough reading and understanding of policy terms, definitions, and meaningful conversations with carriers about what is covered and under what circumstances, can result in a policy that covers the right risks, and a buyer that understands the cost of the policy - and its limits**.

- **Not Now**. We are not mature enough to subscribe to cyber insurance, we just aren't there yet, in terms of our program – In some cases insurers only offer coverage or offer much better rates to organizations who comply with certain standards or security best practices. Subscribing to insurance coverage may help an organization to improve their security posture.

While some losses may be covered under other business liability or errors and omissions coverage, these other policies leave many gaps for losses and expenses stemming potential cyber incidents. Most policies provide for first-party coverage (this means the coverage of losses for the loss or expenses you incur due to a loss of data or other incident) or third-party coverage (expenses you incur when others are affected by an incident that you experience).

**ANALYSIS**. A recent study by RAND, examined 105 insurance policies filed with insurance commissioners from New York Pennsylvania, and California. They found that areas of coverage and areas of exclusion both called controls, were more standard than many commentaries imply, but that there was some overlap between coverages and exclusions. The researchers identified 50 total controls. 15 of them were coverages and 35 exclusions. Furthermore, the way controls were covered or excluded were different for most policies. When examining first-party coverage (coverage of losses relate to those directly suffered by the insured), examples of common costs covered by first-party policies include:

- Costs related to investigating the cause of a data breach or security incident;
- Costs associated with restoring business services;
- Cost of notifying affected individuals;
- Credit monitoring services.

Another similarity across many first-party coverage policies are categories that have specified sub-limits or distinct premiums. Such groups of categories are Personal Data Compromise, Computer Attack or Identity Recovery, and/or Cyber Extortion. The coverage of some topic areas varied greatly between policies. It is critical for buyers for thoroughly read a policy and understand how the terms are defined and under what circumstances specific expenses or losses are covered.

The exclusions overlapped with the coverages. Some policies explicitly exclude costs incurred to correct a deficiency. Various policies defined such costs in different terms. Very few policies covered costs of data extortion or costs resulting from acts of terrorism or acts of war. Those policies that covered extortion further excluded ransom for digital data. This means they only covered ransom to physical assets. One policy limited coverage to data assets.

Third-party Liability Policies cover three main areas: (1) liability to third parties for privacy breaches, (2) liability to regulators for privacy breaches, and (3) liability to third parties for computer system security breaches. Similar to first-party policies, limits are distributed across several categories:

- **Data Compromise** – coverage for defense and settlement costs when a third-party sues the insured due to a personal data compromise;
- **Network Security** - coverage for defense and settlement costs when a third-party sues the insured because of:
    - Breach of third-party business information,

    - Unintended propagation or forwarding of malware,
    - Unintended abetting of a denial of service (DoS) attack,
    - Inability of an authorized third-party user to access the insured's computer system.
- **Electronic Media** – coverage for defense and settlement costs in the event that a third-party claimant sues the insured claiming that the insured's electronic communications resulted in:
    - defamation,
    - violation of a person's right of privacy,
    - interference with a person's right of publicity,
    - or infringement of copyright or trademark.

Third-party liability policies have several areas where coverage is common, but how the item is defined, or the circumstances for coverage, can vary for each policy. Those areas include: computer forensic costs, notifications and additional services to individuals, coverage for PR costs, and other areas.

Exclusions found in third-party liability policies most commonly resulted from other types of incidents such as fraudulent or dishonest acts, errors or omissions, intentional violation of a law, any ongoing criminal investigation or proceedings and payment of fines, penalties, or fees, or criminal activity that is not related to a cyber event. Also excluded were infringement of patents, disclosures of trade secrets or confidential information or violations of securities laws. The exclusions at times also had exclusions. Some matters of physical harm and losses to systems out of the policyholder's control were also excluded. Also, expenses for extortion or from an act of terrorism, war, or a military action were mostly noted as exclusions.

To assess risk, determine coverage and apply pricing algorithms, insurance carriers typically ask anywhere between 10 and 100 questions. The major factors used by the carriers are:

- **Organizational Controls**
    - Data Collection and Handling
    - Outsourcing
    - Incident Loss History
    - IT Security Budget and Spending
- **Technical Controls**
    - Information technology and Computing Infrastructures
    - Technical Security Measures
    - Access Control
- **Policies and Procedures**
    - Information and Data Management
    - Employee, Privacy and Network Security
    - Organizational Security Policies and Procedures
- **Legal and Compliance**

Sadly, there are quite a few litigation cases between insured firms and carriers regarding the terms of coverage. As the legal and regulatory environment evolves, and as cyber incidents and data breaches become more public and frequent, the market and legal environment will continue to evolve and standardize. Equally unfortunate are the high-profile cases such as Target, Home Depot, and others where cyber policies paid as agreed, but provided substantially less coverage than the losses incurred by the insured. In most cases the details of coverage terms or exclusions were at issue. It should be noted that **insurance carriers do not define terms in the same way cybersecurity professionals or businesses define them**. All policies including definitions and terms should be thoroughly read and understood. As policies still vary, many are negotiable. Businesses should take advantage of the ability to choose coverages and tailor policies to specific needs and risks.

In addition to coverage, **businesses should also understand how the carrier will assist during incident response stages**. Some carriers allow the insured to choose their own providers such as forensic experts and law firms, while other carriers will require to be notified first and will provide forensic efforts, legal defense providers, and more. Other carriers have lists of preferred providers whose services are covered by the policy. **The two most important things businesses looking for cyber insurance coverage can do are to conduct a realistic assessment of their own risk posture and seek out policies that provide appropriate coverage.**