
This article brought to you by ***Commercial Investment Real Estate***, the magazine of the **CCIM Institute**.

To read the entire issue or find out more about the Institute, go to **www.ccim.com**.

→

# Cyber Scares

## Protect your business from online security breaches.

by Alan Lyons

On an almost daily basis, cyber criminals successfully breach the security systems and networks of U.S. companies to compromise or steal personal and private information. Cyber attacks are occurring at an unprecedented rate and can result in significant financial fallout for companies. According to Ponemon's 2015 Cost of Data Breach Study, the average consolidated total cost of a data breach is $3.8 million — a 23 percent increase since 2013.

### Data Everywhere

Although large data breaches in the retail, financial services, and healthcare sectors have dominated the headlines, the real estate industry is also very much at risk. For example, last year Essex Property Trust, a California-based real estate investment trust with nearly 250 apartment communities, reported a cyber intrusion that compromised its computer networks containing personal and confidential information.

Property managers, landlords, brokers, and appraisers all maintain various types of private personal data, such as tax returns, bank account information, and Social Security numbers in rental and mortgage applications. Landlords provide portals for tenants to pay rent online using credit or debit cards. Also real estate companies retain employees' personal information.

A data breach can happen to any business, large or small. However, hackers tend to target smaller companies assuming that their network security systems are more vulnerable than those at large companies.

Given this reality, real estate companies can protect themselves by having an up-to-date network security system to safeguard their corporate data. However, no security system is completely fail-safe as hackers continually evolve and become more sophisticated. Therefore, one strategy to offset the financial consequences of a cyber attack is through designated cyber insurance.

### Minimizing Risk

Traditional business liability insurance policies do not fully address online exposures, so cyber insurance can fill that gap. However, a wide variety of policies and levels of protection are available. Here's a breakdown of the typical terminology you'll see when shopping for a cyber policy.

Cyber insurance can provide both first-party and third-party coverage. First-party losses are those sustained directly by the insured company. Third-party losses are those sustained by others who assert claims against the insured company to recover those losses and typically cover the insured against privacy liability and/or network security liability.

First-party cyber policies can cover certain types of data breach costs, including expenses to:

- retain a computer forensics firm to determine the cause and scope of a breach;
- comply with privacy regulations;
- notify and provide credit monitoring services to affected individuals whose personally identifiable information is compromised, including setting up call centers to field inquiries from concerned customers;
- retain legal counsel to respond to regulators; and
- hire public relations and/or crisis management services to restore the company's reputation.

First-party policies can also cover the cost to recreate, restore, or replace the company's lost, corrupted, or damaged software or data. The policy may also cover lost business income when operations are interrupted or suspended because of a security breach. Also available is extortion coverage for payments made in response to a ransom demand to prevent a threatened cyber attack.

### Points to Consider

Here are some of the issues to consider when purchasing cyber insurance.

Andrew Brookes/Glow Images

**What type of data is covered?** Data generally falls into three main categories: personally identifiable information, such as a customer's/employee's name, birth date, email address, Social Security number, and ZIP code; protected health information, such as medical history, including medical records; and payment cardholder information, such as credit card data, including account numbers, expiration dates, and security codes.

**What constitutes a covered data breach?** The policy should cover unauthorized disclosure of data, whether accidental or intentional; unauthorized acquisition of data when the company's data ends up in the possession of an unauthorized third party; and the compromising of data when it is corrupted, erased, altered, or held for ransom.

**What are the applicable limits?** An important consideration is obviously the overall policy limit, but companies should also pay particular attention to whether the policy provides sufficient sublimits for legal, computer forensics, public relations, and/or crisis management expenses.

> Hackers tend to target smaller companies assuming that their network security systems are more vulnerable.

**What are the policy exclusions?** The exclusions in the policy must be read very carefully. For example, an insurer recently filed a lawsuit seeking a ruling that no coverage applies for its insured's data breach. The denial was based on an exclusion for claims "directly or indirectly arising out of, or in any way involving failure" by the insured to implement procedures and risk controls identified in the insured's insurance application and any related information submitted in connection with the application.

With the costs of data breaches rising and attacks on smaller companies increasing in frequency, real estate companies would be wise to invest time and resources to upgrade their network security systems, review their existing insurance policies, research the right type of cyber policy, and analyze the scope of coverage and policy language with an experienced attorney and insurance broker. Once hackers strike, it's too late to turn back the clock on being prepared or handling the business and reputational damage.

**Alan Lyons** is chair of the Insurance and Reinsurance Group at Herrick Feinstein LLP, based in New York. Contact him at alyons@herrick.com.