Cyberthreats are escalating and business trade partners and consumers are insisting on safeguards for their private information. It is vitally important for businesses and their law firms to understand the actions needed to maintain cybersecurity and the insurance coverage necessary to cover the damages from cybersecurity breaches.

In a recent episode of the TV series, "The Good Wife," the fictional law firm was confronted with a cybersecurity threat demanding that $50,000 be paid within 72 hours or all files on the firm's computer network would be destroyed. Drama aside, "ransomware" is not fiction and ranks alongside more established cyberthreats for which cybersecurity insurance should be in place.

The potential liability and damages resulting from a data breach can be so great that companies cannot afford to be without proper insurance and adequate coverage.

Corporate Cybersecurity is under investigation by both Financial Industry Regulatory Authority (FINRA) and the U.S. Securities and Exchange Commission (SEC) who are colle information about the level of security and financial industry preparedness for cyber attacks from registered broker-dealers and registered investment advisers. The SEC expectsto expand its examinations to all U.S. public companies, while FINRA will look into the measures that brokerage firms have in place for securing client data.

Inadequate Cybersecurity has caused a number of prominent Fortune 500 companies to suffer major data breaches recently, resulting in hundreds of millions of dollars in losses.

- Target Corp. in November–December 2013, causing losses of $148 million due to the breaches, only 25% of which was covered by insurance.
- Sony's Playstation Network was compromised in 2011 and again in December, 2014.
- eBay Inc. in May 2014 suffered exposure of confidential data of 145 million customers.
- Sony Pictures in November 2014 had hard drives wiped; threatening messages were sent; and terabytes of private and

commercially sensitive information released to the public domain.

To put the 2014 Sony data breach in some perspective, a Terabyte (TB) of data represents approximately 3.6 million 300 Kilobyte images; about 300 hours of good quality video; or about 1,000 copies of the *Encyclopedia Britannica*. 10 Terabytes could hold the printed collection of the entire Library of Congress. Most desktop computers and many laptops now have 1 or 2 Terabyte drives!

No company can be confident of escaping a large-scale data breach without adequate cybersecurity.

Recently, the U.S. Court of Appeals for the First Circuit, in *Patco Constr*. v. *People's United Bank* (1st Cir. 2012), decided that a bank's online security system was not "commercially reasonable" under Article 4A of the *Uniform Commercial Code* because the security procedures were used in a "one-size-fits-all" manner, rather than being tailored to the particular needs and circumstances of its customers. The appeals court also criticized the bank for failing to take advantage of emerging security technologies.

Cybersecurity Threats/Actors That Companies and their Law Firms Should Understand include nation-state actors, hacktivists, cyberterrorists and cybercriminals. Attacks perpetrated by independent actors can be disguised so that they appear to have been perpetrated by state actors.

Employees' mistakes—such as sending out incorrect data, losing or inappropriately using hardware or becoming victims of phishing scams—have resulted in major cybersecurity breaches. Rogue employees are even more dangerous threats as they often are in a position to easily steal data and even hardware, commit extortion, or sell data to a third party.

Examples of the tools used in recent attacks include spyware, ransomware, PIN skimming and social engineering including phishing, whaling, pretexting or baiting; and exploitation of supply chain vulnerabilities, wireless access points and removable media.

The scope and quantity of threats has multiplied as Bring Your Own Device (BYOD) policies are permitted and often encouraged allowing employees to access company data via mobile devices.

Understanding how threat actors can penetrate a company's information security system is crucial to assessing where a company's cybervulnerabilities lie and obtaining the appropriate cybersecurity insurance coverage.

Commercial general liability (CGL) policies may not insure against cyberattacks and insurers are increasingly willing to litigate coverage issues.

In the aftermath of Sony's data breach, Zurich American Insurance Co., commenced a lawsuit seeking a declaratory judgment that it was not obligated to insure Sony for losses relating to its cyberattacks. The court agreed.

The Current State of Cybersecurity Insurance

The proliferation of cyberattacks has encouraged insurance companies to write specific cybersecurity insurance policies. Premiums for cybersecurity insurance totaled $1 billion in 2012 and $1.3 billion in 2013.

Types of Coverage

Virtually all of the major insurers offer some type and kind of cybersecurity insurance including coverage for not just the direct losses, but data breach/privacy crisis management expenses related to a cybersecurity incident including investigation, remediation, data subject notification, call management, credit checking for data subjects, legal costs, court appearances and regulatory fines. Among the different types of insurance being offered are

- Business network interruption which covers loss of net profit caused by a material interruption to the insured's network due to a cyberattack or a network security breach.
- Multimedia/media liability resulting from defacement of a website, infringement of intellectual property rights, or negligence relating to electronic content.
- Extortion liability.
- Network security liability covering the third-party damages resulting from denial of access to a system, costs related to data stored with third-party suppliers and costs related to the theft of data on third-party systems.
- Injury to Reputation.

- Conduit injury resulting from damages to systems affected by breach of the insured's system.
- Disclosure injury resulting from damages to individuals caused by the unauthorized access of their private information held on the insured's system.

Conclusion

Failure to obtain cybersecurity insurance against the risk of data breach leaves companies exposed to serious and perhaps even imminent financial, legal and reputational risk. Obtaining appropriate insurance coverage is an important part of a company's cybersecurity plan. You should avoid being left alone to deal with the consequences of complex and expensive cybersecurity breaches.