HINSHAW

Alerts

Best Practices - Annual Cyber Insurance Reviews

April 28, 2015
Insurance Coverage Alert

Cybersecurity is not just as an IT issue but an enterprise risk management issue. As with any major business risk, companies should consider cybersecurity insurance as a way to transfer risk and mitigate potential losses.

The cost to respond to a cyber event can be expensive. In fact, the average cost is higher in the U.S. than anywhere else. According to a 2014 Ponemon Institute report, U.S. companies incur an average total cost of $5.85 million per data breach, the highest average cost of any country.

This figure is even higher for heavily regulated entities such as banks. Companies in the financial services industry spend $206 per impacted record, significantly above the overall mean of $145 per record.

Cyber events also take a harder toll on a bank's reputation. In relation to retail or public sector companies, financial services organizations tend to have an abnormally high percentage of customers switch companies as a result of a breach.

Because a significant cyber event could impact a company's financial wellbeing, at least once a year, businesses should evaluate existing insurance coverage for cyber-related risks. For those companies that already have cyber policies, a review could reveal gaps in coverage. Changes in risk tolerances also might require changes to existing policies. And since the cyber insurance market is evolving, all companies – including those that have not yet purchased cyber insurance – might find new products that make this insurance a more attractive risk management tool.

Businesses should not rely upon traditional liability or first-party property policies for cyber-related risks. Traditional insurance policies cover losses from bodily injury or from damage to tangible property. Cyber events, by contrast, involve the loss of or damage to intangible assets such as data or computer software. This type of loss does not fall squarely into any traditional coverages.

Some policyholders have obtained coverage for data breaches under the "personal and advertising injury" prongs of standard commercial general liability policies. This offense-based coverage provides protection for certain enumerated torts such as defamation, false imprisonment, and invasions of privacy rights. However, insurers typically have strong defenses to data breach claims and, in many instances, have been able to defeat coverage.

Attorneys

Timothy M. Sullivan

Service Areas

Fidelity

Surety

To close the door on the potential coverage for cyber events, insurers recently expanded cyber-related exclusions in traditional policies. As a result, policyholders will have to turn to specialty insurance to obtain coverage for this risk.

Businesses may buy standalone cybersecurity policies or riders. Cyber insurance tends to provide targeted coverage for discrete harms, in which separate coverage grants address each different type of loss or damage. For this reason, businesses should carefully evaluate the risks they face and ensure that their cyber policies or riders actually cover those potential losses.

Third-party cyber risk policies protect against liability and other costs arising from data breaches. Data breaches result in a variety of losses, not all of which are covered under every cyber liability policy:

- **Breach notification costs** – Federal law requires financial institutions to provide consumer notice if institutions determine that misuse of consumer information "has occurred or is reasonably possible." Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12 CFR Parts 568 & 570. These costs can be substantial.
- **Credit monitoring costs** – Federal law does not currently require banks to pay for credit monitoring services for potentially affected customers – banks only must recommend that affected consumers take steps to monitor their credit. Nonetheless, to mitigate reputational harm from a data breach, financial institutions should consider offering credit monitoring services free of charge. Cyber insurance helps defray this cost.
- **Liability and defense costs** – Due to notification and reporting requirements, knowledge of a data breach quickly becomes public. This often results in litigation. A cyber liability policy would cover defense costs and damages arising from these lawsuits.
- **Civil fines and penalties** – In addition to damages – such as consumer losses due to identity theft – a data breach could result in penalties and fines. Not all cyber insurance applies to these types of losses, which may require special coverages.
- **Regulatory proceedings and lawsuits** – In response to a breach, a government agency could initiate an inquiry into a company's data management or file a lawsuit. Unless a policyholder buys coverage for this particular risk, most cyber policies probably would not cover costs to respond to government actions.
- **Crisis management** – Many businesses have contingency plans in the event of a breach, which might include media campaigns designed to reduce reputational harm. Cyber insurance can help fund these initiatives.
- **Excess or umbrella coverage** – Cyber liability policies generally have "burning limits," meaning defense costs erode limits. Because defense costs can burn through coverage quickly, companies should consider buying umbrella or excess cyber liability insurance.

Businesses can also buy first-party insurance for cyber-related losses. The market for first-party cyber insurance is not as developed as that for liability coverage. Many businesses have found that first-party insurance either does not provide the protections they want or that the cost is prohibitive. As the cyber insurance market evolves, and as insurers get better at underwriting the risk, more affordable products could come onto the market.

First-party cyber insurance protects the policyholder against business losses or costs to repair or restore lost data, information, or software. Like third-party insurance, first-party coverages can be tailored to a business's specific needs:

- **Data restoration** – A cyber attack could cause data loss or make information inaccessible. A first-party policy would cover costs incurred to restore this data.
- **Forensic investigation** – Restoring data is not the only potential cost. In the event of a cyber attack, companies will incur significant forensic costs to determine the source of the attack, assess the scope of damage, and repair any damaged or infected software.
- **Business interruption losses** – A network failure, even for a short period, could result in significant business losses. If physical conditions caused the failure, such as damages from a fire, a first-party property policy might cover business interruption losses. However, a property policy would not cover a network failure due to a cyber attack or malware. For that risk, a company needs cyber insurance.

- **Contingent business interruption losses** – Many institutions rely upon third parties to provide services or for network support. This is often the case with cloud computing vendors. When the computer systems of those other companies go down, business losses may result. Some cyber policies will provide business interruption insurance for this contingency, even if the policyholder's own systems are unaffected.
- **Cyber extortion** – A business might receive credible threat that an unknown third party will cripple the company's network or access confidential data on servers. The company could decide to make an extortion payment to the group making the threat. A cyber extortion policy could cover that payment and other costs incurred in responding to the threat.

Cyber events come in many forms – data breaches, malware, lost or stolen laptops with confidential data, denial of service attacks in which systems are overloaded with traffic, and cyber extortion. Because the potential threats are varied, insurance for these risks is varied as well.

Cyber insurance should be an integral part of any enterprise risk management plan. But before buying any cybersecurity policy, companies should scrutinize the particular risks facing their businesses and buy insurance tailored to their own business needs and risk tolerances.