Market Blueprint: Cyber Insurance

Debunking Cybercrime Misconceptions

With the explosive growth in e-commerce, cloud computing, connected devices, autonomous vehicles, and manufacturing automation, digitized information is quickly becoming the world's most valuable commodity and a treasure trove for thieves. In many ways, data and automated system controls are the new "private property" and cybercrime is like a warehouse fire. As more business infrastructure connects digitally, it becomes even easier for cyber criminals to intercept and manipulate data and systems for ill intent. In fact, two ransomware cyber attacks have occurred since you began reading this article (at a rate of one every 22 seconds and a total cost to the effected companies of $2 billion so far in 2019 alone).

Ninety-five percent of cyber attacks against companies are initially triggered by simple human error. Unlike machines, people are vulnerable to psychological trickery. Hackers directly target people inside a company, and by tricking them into opening emails or revealing insufficiently secure passwords, they then use tools like spyware and malware to take control of systems from anywhere in the world. As the stakes get higher, cyber criminals continually modify their tactics to thwart capture.

In spite of this growing prevalence, a surprising number of organizations fail to understand the true scope of the threat and are therefore vulnerable to potentially catastrophic losses should they fall victim to a cyber attack themselves. According to a 2019 study by the data-analytics company FICO, 24% of U.S. executives surveyed admitted their firm has no cyber security insurance. The study also revealed that 68% of those surveyed believed their existing cyber insurance was not broad enough to cover the entire scope of their digital risk. Case in point—in a few recent high-profile cybercrime cases, the victimized companies believed they had cyber insurance, but instead had less-robust "cyber as a peril" bolt-ons to traditional property insurance policies, which had very small sublimits of coverage insufficient to cover the scope of their damages.

Here are three main reasons why organizations underestimate—and underinsure—their cyber risk, and why they should reevaluate their position moving forward:

MYTH #1

My IT department assures me our servers are impenetrable.

The reality is that if you have employees with email, wireless devices and network access, you run the risk of a cyber attack. In spite of state-of-the-art password management, server security and encryption, each employee is a potential path for cyber attackers to access directly into your systems and databases. Instead of attacking highly secure servers head on, hackers go for the weak link—the people who use them. Once an unsuspecting employee opens a phishing email, and malware is placed on your servers, even the best IT teams will struggle to contain what cyber security experts liken to a forest fire.

A study issued in November 2018 by Ponemon Institute reported that 59% of 1,038 companies said they had experienced a data breach caused by one of their vendors or third parties.

In March of 2019, Norsk Hydro ASA, one of the world's biggest aluminum producers, suffered production outages after a phishing scheme duped an employee and the resulting LockerGoga ransomware hijacked their worldwide manufacturing control software. The ransomware switched all of Norsk Hydro's smelting plants into manual mode, and it took the company several days to ascertain the scope and root cause of the problem. The attack cost the company $52 million and forced them to postpone reporting first quarter earnings by five weeks while they restore reporting, billing and invoicing systems. Fortunately, Norsk Hydro carried cyber insurance which is helping cover their losses from the attack.

Could your business absorb the loss of production output for days or even weeks? Who would help you quickly find and resolve such an attack?

MYTH #2

We don't collect credit card data, so there's no risk.

While major consumer brands like Delta Airlines, Macy's and Best Buy have made headlines for consumer credit card breaches in recent months, large companies are not the only targets for attacks. Actually, in 2016 43% of all cyber attacks were conducted against small to medium-sized businesses. Most often, smaller companies fall victim to thieves posing as legitimate customers who place product orders on credit for shipment to bogus locations. Considered by insurance claims adjusters to be a "voluntary parting," these sorts of fraudulent incidents are not covered by traditional property insurance policies.

How easy would it be for your organization to absorb the financial loss that arises when an unsuspecting sales administrator ships (or voluntarily parts with) five orders of $50,000 each to a fake address with zero chance of receiving payment?

MYTH #3

Cyber insurance is too expensive and hard to cost-justify.

By 2020, cybercrime experts predict that the average cost of a single data breach (in lost revenue, market value, employee productivity and legal fees) will exceed $150 million. According to a Microsoft study, the average cost to a middle-market firm from a cyber attack is currently $430,000. The business interruption caused by these digital attacks is not covered by traditional property insurance.

In contrast, cyber insurance, which covers damages, liability and recovery costs resulting from cyber attacks, is a relative bargain. When you consider the breach-support services provided along with these policies (including negotiators and forensics experts), and even reputational management services (like covering the cost of hiring public relations firms) their value far exceeds the cost.

Even if your business could absorb a $430,000 cyber attack, how well would you weather the longer-lasting impacts to your reputation and the loss of customer trust?

Not If, But When

Given how valuable data and automated systems are to your business, a holistic approach to assessing, mitigating, and correctly insuring against cyber risk is critical, and will only increase over time. You need an insurance partner who is able to assess the full scope of your exposures, and build the most comprehensive program to reduce your total cost of cyber risk. The seasoned Team of Experts at Alper Services will audit your cyber exposure and make recommendations for the appropriate cyber insurance coverage, to ensure your business is as resilient as possible to an inevitable cyber attack.

Alper would like to help you gauge your cyber exposures, and importantly, review where you have the opportunity to bolster your protection. Click HERE to complete a short questionnaire that will allow Alper to assess your risk.

To answer your immediate questions regarding cyber risk, please contact Bobette Puckett at BPuckett@AlperServices.com.