Should Retailers Purchase Cyber Insurance to Mitigate Ransomware Risk?

According to a recent report, 44 percent of retail organizations suffered ransomware attacks in 2020. And attacks increased in 2021. With the average cost of a single ransomware attack reaching nearly $2 million, many retail businesses have looked to cyber insurance to offset the risk.

But the choice of whether or not to purchase cyber insurance requires careful consideration. As the threat landscape changes, insurance companies have also had to change their approach. Cyber insurance can prove costly. And it does not prevent attacks, merely helps recovery. In fact, some experts warn that purchasing cyber insurance can even invite attacks.

Understanding Cyber Insurance Basics

A standard business owner insurance policy does not cover cyberattacks. However, organizations can purchase specific cyber insurance to protect against the damage that results from a cyberattack.

Cyber insurance coverage varies widely from company to company. In general, policies will cover some combination of the expenses and losses initiated by a ransomware attack. For instance, this can include ransomware payments, data recovery, expenses related to business interruption, cost of remediation, legal fees, and regulatory investigations.

Uptick in Ransomware Attacks Means Changes to Insurance

As ransomware attacks increase, and as they become more costly, the nature of cyber insurance is changing. Two major trends have emerged. First, coverage is proving much more expensive than before, with premiums increasing by 10 to 50 percent.

Second, insurance companies are now requiring organizations to demonstrate a strong cybersecurity posture. That is, they must show that they have preventative measures in place in order to purchase coverage. These mandates often include multi-factor authentication (MFA), as well as endpoint detection and response (EDR) systems.

Additionally, cyber insurance policies may now include certain exclusions and coverage limitations. For example, last May, European insurance giant AXA decided to drop ransom payment coverage from new cyber insurance policies. Other insurance companies may follow suit.

What to Look for When Choosing Cyber Insurance

Because of these changes, organizations choosing to purchase cyber insurance need to do their research and carefully review policy language. Policies should cover a wide variety of threats, using broad terminology.

Coverage should certainly include specifically accessing, misusing, or selling digital assets. Threats covered could also include actions such as altering software or interfering with the organization's website. Additionally, the policy should cover introduction of malicious code, restriction of access and threats to disclose data or disrupt business.

In addition to the coverages, understand the insurance company's approach to ransom payments, as well as the policy's definition of extortion. That is, does the policy require an explicit threat to sell corporate data in order to trigger insurance coverage? Too often, businesses purchase insurance without looking closely at the specifics of the policy.

Cyber Insurance as Part of Comprehensive Strategy

Cyber insurance can play an important role. However, it will not prevent an attack. Instead, it should form just one part of an overall cybersecurity strategy. In fact, as indicated, organizations with a strong security posture will likely find it easier and cheaper to purchase insurance. And strong security measures make an organization a less attractive target.

Start with basic cybersecurity best practices, such as MFA and email encryption. Implement automated backups and test them regularly. And regularly conduct risk assessments and penetration testing to identify vulnerabilities, adjusting security measures accordingly.

Retail cybersecurity professionals offer the tools and expertise you need to tailor a cybersecurity solution to meet your business needs. The consultants at Messaging Architects deliver a range of critical services, beginning with comprehensive risk assessments and email filtering.