For Oklahoma Bankers Association – June 2016
issue Rayleen M. Pirnie, AAP
RP Payments Risk Consulting Services, LLC

Business Client Article

Suggested target audience: Small to Mid-size Business Customers

Title: Debunking Cybersecurity Insurance Myths

Cybercrimes continue to run rampant, stealing millions of dollars from businesses every year. How would your business recover if an attack occurred?

According to the National Cyber Security Alliance, about 70% of cyberattacks target small to mid-sized businesses (SMBs). Unfortunately, many SMBs don't recover; about 60% of breached SMBs go out of business within 6 months of the attack. Most SMBs outsource services, which puts you at greater risk.

As the volume of electronic data collected and stored by businesses increases, the number and extent of cyber-losses do as well. We are an inter-connected, online world. While it's necessary for our businesses, these practices carry many risks. In the security world we have a saying: it's not a matter of IF you are breached, just a matter of when and how significant the damage is. Meaning, your business will very likely be breached. No matter how small or rural you are, criminals can find you online. So we need to change our thinking from a solely "prevention" standpoint to one that blends mitigation with recovery.

Before you plan to turn to your insurance agency to recover from a cyber-related loss, you need to make sure you are truly protected. Businesses are frequently finding that while they have "cyber-insurance" provisions, they are not covered for the type of attack they encounter. Other businesses, unfortunately, either believe they are already covered or that they have no need for cyber-policies. In this issue, we're discussing some common myths of cybersecurity insurance.

Myth 1: Our business has a general liability policy which protects us from claims of "property damage" and "consumer harm" so we are covered if we have a cyber-attack.

Reality: Back in 2001, the Insurance Standards Office (ISO) of the United States removed "electronic data" from the definition of "property damage" found in typical general liability policies. The clarification was due to the fact that one businesses insurer would pay out on a data breach, but another would not, even though both claims and policies were very similar. Two agencies issuing similar policies were interpreting the language differently. This was largely due to state courts interpreting the definition of "electronic data" differently. So the ISO issued a clarification for insurers and policy holders. So in short, your general policy will not cover breached data.

Talk to your insurance provider and ask cyberattack specific questions. Things that commonly happen to businesses like yours or that the FBI classifies as a significant threat against U.S. businesses. Learn if you will actually be protected in these cases. Before adjusting an existing policy or adding a new one, have an attorney who is educated in cyber risks and cybersecurity insurance review the policy before signing.

Myth 2: All cyber insurance policies are the same.

Reality: Cybersecurity policies are not all created equal. It's important to ask questions and make sure you are getting the coverage you expect. The recent case of AFGlobal Corp. demonstrates how an entity could assume a certain type of cybercrime related loss would be covered under their policy, yet the insurer denies, claiming the incident is outside the scope of coverage.

The scope of coverage can vary drastically among products offered by insurance carriers. There also appears to be inconsistency in terminology among different insurers, meaning a term may mean one thing in one policy, and something different in another policy.

Policies for losses related to a breach of customer or employee privacy is pretty easy to find; however, policies covering losses related to lost revenue, stolen assets, hardware and software replacement, etc. is much more difficult.

Premiums is also something that varies widely. Gartner, Inc., recently reported that cyber insurance premiums range from $10,000 to $35,000 for $1 million in coverage. Depending on the insurers underwriters and understanding of cyber risks, there can be a pretty significant difference in coverage and premiums, as much as 25% in premiums charged by two carriers for the same risk.

Myth 3: We have a cybersecurity insurance policy, so we're completely covered.

Reality: Not necessarily. What does your policy cover? I've worked with businesses before who thought they were covered, only to have a cyberattack occur and they quickly learned differently. I encourage, before signing up for any cybersecurity policy, have a lawyer familiar with these types of policies review it first. If you already have coverage, it's a good practice to review the policy and terms before renewing.

According to the National Association of Insurance Commissioners, cyber liability policies might include one or more of the following types of coverage:

- Liability for security or privacy breaches. This would include loss of confidential information by allowing, or failing to prevent, unauthorized access to computer systems.
- The costs associated with a privacy breach, such as consumer notification, customer support and costs of providing credit monitoring services to affected consumers.

Note: this may or may not include covering costs associated with the theft of employee data.

- The costs associated with restoring, updating or replacing business assets stored electronically.
- Business interruption and extra expenses related to a security or privacy breach.
- Liability associated with libel, slander, copyright infringement, product disparagement or reputational damage to others when the allegations involve a business website, social media or printed media.
- Expenses related to cyber extortion or cyber terrorism. Note from author: this is a significant problem for businesses of all sizes right now. Make sure your policy covers ransomware losses. If your business elects to pay the ransom to recover your systems, you also need to understand if you policy will help you recover some of that loss. Many do not.
- Coverage for expenses related to regulatory compliance.

Cyber-attacks present a lot of different threats and damages; your business should decide what you need to protect and then identify a policy that covers those areas. It's more than just signing up for a blanket-style policy.

Myth 4: We can just add cyber liability provisions to our existing policy.

Reality: A cyber-attack is a costly proposition for anyone, and your insurance agency isn't going to take this policy lightly. In fact, many insurers won't even provide a policy until your business has successfully demonstrated sound risk management practices applied not only to your network and how you store consumer data, but also to how you secure your accounts (i.e. security controls for sending wire transfers, payroll files, etc.).

Insurers will likely want to see your disaster response plan and your cyber incident response plan. The insurer will be keenly interested in how employees and third-parties are able to access data on your network and systems. At a minimum, the insurer will want to know how you secure data (i.e. anti-virus, security suites, anti-malware security, encryption of confidential data at rest and in transit, etc.)

Myth 5: Cybersecurity insurance is too expensive for my business.

Reality: A cybercrime is far more expensive. The 2014 Poneman Study found that the costs and losses associated with data breaches is increasing. The companies involved in the study reported an average loss of $201 per exposed record, and an average of 29,087

records per breach, with an average loss of $5,846,487 per breach for the companies studied.

About the Author

Rayleen is the founder and owner of RP Payments Risk Consulting Services, LLC. based in Missouri. She is a nationally recognized speaker whose educational programs provide valuable, actionable strategies for financial institutions and businesses on topics ranging from payments risk management to information security. She is the author of several payments risk and fraud blogs geared toward helping organizations recognize threats and protect themselves from loss.