WHITE PAPER

GILLIAM SECURITY

Cyber Insurance:
To Get Paid or Not Be Paid

Understanding when and what type of cyber liability insurance will help you the most.

So you have bought cyber insurance. Let's take a deep breath knowing that you can be assured that you will not be out millions of dollars should your legal team announce your organization has been breached. Or maybe your organization will hear the words, "we are unable to cover your expenses."

Unfortunately, the latter is a more frequent answer. Cyber liability insurance, like that of other insurance policies, are very specific to the coverage provided. In reviewing your organization's policy, here are a few things to audit and verify within the policy.

Let's create a scenario to help us understand what our best protection is and what will be minimize an organization's cyber security risk posture:

You are the Chief Technology Officer of a company called "ACME Widgets." Your infrastructure for ACME Widgets is on a hosting provider called "ACME Hosting." ACME Hosting has cyber liability insurance policy.

Today your boss had a meeting with the finance team that has asked to bring another product into the organization to help with hosting. After that meeting, you had a meeting with your boss where you were asked the following questions:

- What type of cyber insurance do I have today and will this cover us for our hosting at "ACME Hosting"?
- What kind of cyber insurance will minimize our risk of using "ACME Hosting"?
- What kind of cyber insurance will minimize our risk of my network within "ACME Widgets"?

Types of Cyber Liability Insurance

To answer these questions, we must first understand what is "first-party" cyber liability insurance and what is "third-party" cyber liability insurance?

- First-Party Cyber Liability Insurance – Think of "we have cyber liability insurance but it won't help you!"

  This type of insurance is very helpful to the company itself that has been breached but it is not helpful to you if you are the client of this company.

- Third-Party Cyber Liability Insurance – "I want insurance to protect me from you!"

  This type of insurance helps with the legal expenses of ACME Widgets when ACME Hosting or one of ACME Widgets third parties has a security incident such as a breach.

Protection from the Impact of a Security Event

Now that we understand the difference between First-Party Cyber Liability Insurance and Third-Party Cyber Liability Insurance, let's look at which will minimize the impact of a security incident:

First-Party cyber liability insurance will help with activities such as:

- Customer notification in the event of a security incident such as a breach
- Providing customer protective controls in the event of a security incident such as a year of credit monitoring
- Potentially expense reimbursement for business interruption and lost revenues due to resources working the security breach
- While not encouraged, paying a ransom if you are attacked by ransomware. Why not encouraged? By paying a ransom, one must ask the question of did the organization fix the vulnerability that caused the ransomware attack?

Each of these activities can potentially be included in the contract of your service provider, minus business disruption. That said, see if the contract for ACME Hosting includes such coverage.

Third-Party cyber liability insurance will help with activities such as legal expenses that may result in you suing ACME Hosting.

Reviewing the Contract of the Provider

Prior to your next meeting with your Chief Technology Officer, consult your legal team to share the contract, prior to signing, with your legal team to understand what the right balance of insurance is.

Secondly, be sure to explain both first party and third party security risk to your Chief Technology Officer as both may adversely impact the organization differently.

Last, before sending the question to your SaaS, PaaS, or IaaS provider, always ask what type of cyber insurance the provider has.

Need help performing a third-party risk assessment? Contact Gilliam Security today and we can help you out!

NOTE: This article is in no way a substitution for legal advice, rather only based on lessons learned.

Why Gilliam Security?

Gilliam Security has recognized consultants from major fortune 500 companies with certifications such as the CISSP, CISM, CISA and CRSIC. Each consultant also has experience in building the information security, as well as privacy, function from inception to maintaining operations.

Contact Us Today at sales@gilliamsecurity.com