CYBERSECURITY INSURANCE Guidelines

CYBER CIC

Presented by: Carmine Cicalese

www.cybercic.com carm@cybercic.com 717.706.3832

We Designed This Guide to Make and Keep You Insurable

At CYBER CIC, we like to say that the first important cybersecurity decision a business owner makes is to choose a great information technology, or IT, partner who can establish the essential technologies to protect the business.

This person can provide the basic technologies like patch updates, anti-virus, and multi-factor authentication to provide your basic business security. In a bit, we'll circle back to IT to discuss its relevance to cyber insurance.

When it comes to cybersecurity and cyber insurance, the most popular statement I hear from small- and medium-sized business owners is "I don't need cybersecurity expertise; I have cyber insurance."

“I don’t need cybersecurity expertise; I have cyber insurance.”

www.cybercic.com

CYBER CIC’s reply: “Great! Do you know what your minimum diligence requirements are to collect if you are breached?”

Owner: “Huuuuhhhh???”

CYBER CIC: “Please send me your policy and underwriting documents, so we can have a talk.”

Let’s Talk About Risk + Insurance

Risk is a simple formula: Risk = likelihood X impact

BY ITSELF, CYBERSECURITY INSURANCE DOES NOTHING TO REDUCE THE LIKELIHOOD OF A BREACH. Zero. Zilch. Nada. Goose Egg. Donut. Doughnut. Nothing. Nuthin’. No thing.

CYBER INSURANCE MISCONCEPTIONS

Business studies estimate the average cost of a cyberattack on small and medium businesses ranges from $25,000 to $3 million with an average claim of almost $350,000.

While cyber insurance may reimburse you - minus the deductible - for reconstituting your data, it might not cover the cost of lost business, compliance fines, legal fees, operational delays, and reputation damage unless you purchased those coverages. In nearly 25% of all cyber attacks, exclusions limited full insurance payout. However, the more blocks you can check responsibly on the cyber insurance underwriting request, the more you reduce the likelihood of a breach AND the more you reduce your cyber insurance premium.

Not all insurance brokers ask the same questions. Not all IT companies offer the same services. Still, CYBER CIC published this handy guide to show business owners what to expect when applying for cyber insurance and what essential IT support you should expect from your IT partner. We said we'd come back to that important IT relationship. Let's dig into it.

CYBER CIC

Average Cost of Cyberattack for Small to Medium Sized Business

$350,000

UNDERWRITING

Basic

For starters, look at what Cybercic categorizes as basic underwriting questions. At an absolute minimum, your IT partner must be capable of providing these services. If not, find a new one fast.

- [ ] Patch management procedures
- [ ] Multi-factor login for privileged access
- [ ] Remote access limited to VPN/RDP
- [ ] Media and website content controls
- [ ] Valuable/sensitive data backup procedures
- [ ] Data encrypted at rest and in transit
- [ ] Updated, active anti-virus deployed on all computers and servers
- [ ] Updated, active firewall technology
- [ ] Updated, active EDR or intrusion detection technology
- [ ] Annual individual cyber awareness training

Advanced

The next batch of questions we characterize as advanced questions. Somewhere in here, you may find that your IT partner, unless it is a cyber-first IT provider like a managed services and security provider (MSSP), cannot provide a particular service. This is when a company like CYBER CIC helps fill the capability gap. Capabilities like email filtering and phishing exercises can often be filled best by the IT provider…if it is willing to expand its scope. By the fifth bullet, intrusion protection technology, the list may be surpassing the IT team's capabilities. Unless the IT provider is an MSSP as mentioned earlier, contact Carm.

- [ ] Email filtering
- [ ] Email phishing excercises
- [ ] Active directory/service accounts
- [ ] Data and network segmentiing
- [ ] Updated, active intrusion detection technology
- [ ] Procedures to test or audit network security controls
- [ ] Business continuity plan
- [ ] Disaster recovery plan
- [ ] Incident response plan
- [ ] Third party risk management - diligence service providers
- [ ] A person or department responsible for information security

Now Let's Ask Some Compliance Questions

Does your IT provider know how to handle these?

Most IT companies can handle PCI-DSS, but what about other compliance standards?

Sample Compliance Questions:

Is the Applicant currently compliant with Payment Card Industry Data Security Standards (PCI-DSS)?

- Yes ☐
- No ☐
- N/A ☐

Is the Applicant HIPAA compliant?

- Yes ☐
- No ☐
- N/A ☐

Many other compliances exist, like CMMC or COSO, which may or may not be on the underwriting questionnaire.

Who is going to help you but a cybersecurity company? Call us.

Last part and the uncomfortable part for those who have been breached.

Confession.

If your company has been breached, you might want a cybersecurity professional to assist in explaining your position and what you've done to remediate. Contact Carm.

CYBER CIC

Sample Data Loss Questions

In the past 3 years, has the Applicant:

(a) experienced a network or computer system disruption due to an unauthorized system actor or

(b) received any complaints, claims or been subject to litigation involving legal damage from the Applicant's customer's ability to rely on the Applicant's network?

YES ☐ NO ☐

Is the Applicant or any person proposed for this insurance aware of any fact, circumstance, situation, event or act that reasonably could give rise to a claim against them?

YES ☐ NO ☐

NEXT STEPS If any question is answered Yes, contact CYBER CIC.

Last thing. Did you know that if you are breached you should expect to cease operations on your network?

Most policies require the insured to notify their insurance carrier upon a breach or some other qualifying covered event as part of your incidence response plan. Your insurance carrier will have a process and points of contact to help your response team to manage the situation. Depending on the event, the insurance carrier may direct you to not touch anything on the network until the source of the event is idenditifed and can be effectively remediated.

Are you operationally prepared for that scenario? Does your policy cover that operational loss or reputational damage? Contact Carm.

We hope you found this guide useful for understanding the layers of cyber insurance.
Our goal is to help you decrease the likelihood of a breach AND reduce your cyber insurance premium at the same time by using a cybersecurity company like CYBER CIC.

Connect with me on LinkedIn

CYBER CIC

carm@cybercic.com
717-706-3832