Cybersecurity Strategies: Safeguarding Your Organization in the Digital Age

June 7, 2023

Cyber, Property & Casualty, Risk

Derek Laczniak

Director of Manufacturing & Distribution Practice
Partner

Every organization faces cybersecurity risks that could reveal sensitive information and wreak havoc on their business continuity plans. Even smaller businesses are no exception.

No matter the size, organizations should be aware of evolving cyber risks, risk management solutions and the tools available to help prevent cyber-attacks.

Managing the risk of cyber-attacks involves three guiding principles.

1. Adopt an approach of continuous technical improvements to an organization's IT infrastructure with the right cybersecurity tools.
2. Focus on organizational preparation to respond effectively to a cyber incident.
3. Manage risk through the use of risk transfer contracts like cyber liability insurance.

1. Cybersecurity tools

When it comes to choosing what IT security tools and philosophies to deploy in a crowded marketplace, every organization needs to decide what works for them, and what is the most cost-effective. Some of the best decisions IT teams can make do not necessarily come with the highest price tag.

Zero trust architecture

The first thing that should be considered comes at no cost to the business, and that is a "zero trust architecture." Zero trust is not a software product, but rather an all-encompassing philosophy that may dramatically reduce the potential and impact of a cybersecurity incident. Put simply,

> "Zero trust assumes that no user or device can be inherently trusted, and access to resources is granted based on continuous verification that the access has a purpose and a need."

If taken seriously from the top of a organization down to the bottom, this philosophy may reduce the potential impact of attacks because users have access only to information that they need.

In addition to the adoption of zero trust, there are some affordable software solutions that could dramatically reduce the potential for cybersecurity incidents.

Multi-factor authentication (MFA)

MFA has become a buzz word over the last few years as cyber-attacks have increased. MFA is a simple tool that uses an out of band authentication (normally using a text message or push notification on a cell phone) to ensure that a log-in is

being performed by the intended individual. The use of MFA ensures that a bad actor cannot gain unauthorized access simply by having a stolen username or password. MFA solutions are available for free, or they can be purchased. This may be the easiest and least expensive solution for companies to implement to reduce potential cyber-attacks.

Endpoint protection

Endpoint protection is a "catch all" term for a virus monitoring tool. However, it's not the spam ware software that was preinstalled on laptops years ago. Today, they're state-of-the-art tools. Ten years ago, virus monitoring tools had to be "told" what to look for, which limited the ability of the software to evolve as newer attack techniques came out. Tools these days integrate artificial intelligence (AI), so the software looks for any anomalies, not just what it is "told" to look for.

Consistent employee training

Another important solution that could reduce the risk of cyber-attacks is employee training. It is well documented that most incidents are a result of phishing attacks on individual users. It is therefore incredibly important to keep security training at the forefront of employees' minds so they not only know how to spot phishing attacks, but they are constantly reminded that the risk is out there.

2. Incident response plans

"The best offense is a good defense" is the age-old adage that can be applied to many areas of business. That said, sometimes the best defense is just not good enough to prevent a cybersecurity incident from happening. It's important that businesses also plan and prepare for what to do when a security incident happens. Cybersecurity incident response plans are not the same as business continuity

plans because the response for a cybersecurity incident is so unique and requires different steps.

The most important component of an incident response plan is knowing what to do when a security incident occurs. Incident response plans don't have to be more than a few pages, but they should clearly outline who has what responsibilities in the initial critical hours of an attack. Among other items, these plans outline how to communicate within your organization, what outside service providers are appropriate to use and how to communicate with stakeholders. Once completed, they should be tested annually through a practice exercise where the incident response team simulates a security incident.

M3 OFFERS THIS 10-STEP GUIDE TO MITIGATE THE IMPACT OF A RANSOMWARE ATTACK

3. Cybersecurity insurance

The last principle for managing cybersecurity risks is to find the appropriate risk transfer insurance policy. Due to the potential for expenses associated with cybersecurity incidents, organizations may need to offset this potential loss with an insurance contract. The cyber liability insurance marketplace has been around for over a decade, which is a relatively short amount of time in the insurance industry. But it has gained widespread acceptance in the last five years due to the dramatic increase in attacks.

Due to the increased demand for cyber liability insurance policies, the marketplace has exploded with different options and products. Unlike other types of insurance, cyber liability policies are unique and often use different terms and coverages.

When selecting an insurance policy for an organization, be sure to understand who the cyber insurance carrier is. Because cybersecurity exposures are always changing, it's important to partner with an insurance carrier that has proven

experience with your industry and the financial solvency to pay for claims, even in the worst of times.

Due to the complexity in the underwriting process, understanding all the terms, conditions and exclusions present in these policies is critical. That's why it's important organizations partner with insurance experts to match their exposure profile with the right insurance carrier that may provide coverage that meets their risk management needs.

Unfortunately, cybersecurity threats are part of the business landscape today and will be for some time. The pursuit to reduce the risk and prevent cybersecurity attacks for your business will be an ongoing challenge.

While not a guarantee, following these three guiding principles may help keep your organization less exposed to a cyber-attack and better prepared to respond when an incident occurs.

BACK TO INSIGHT CENTER

Related Content