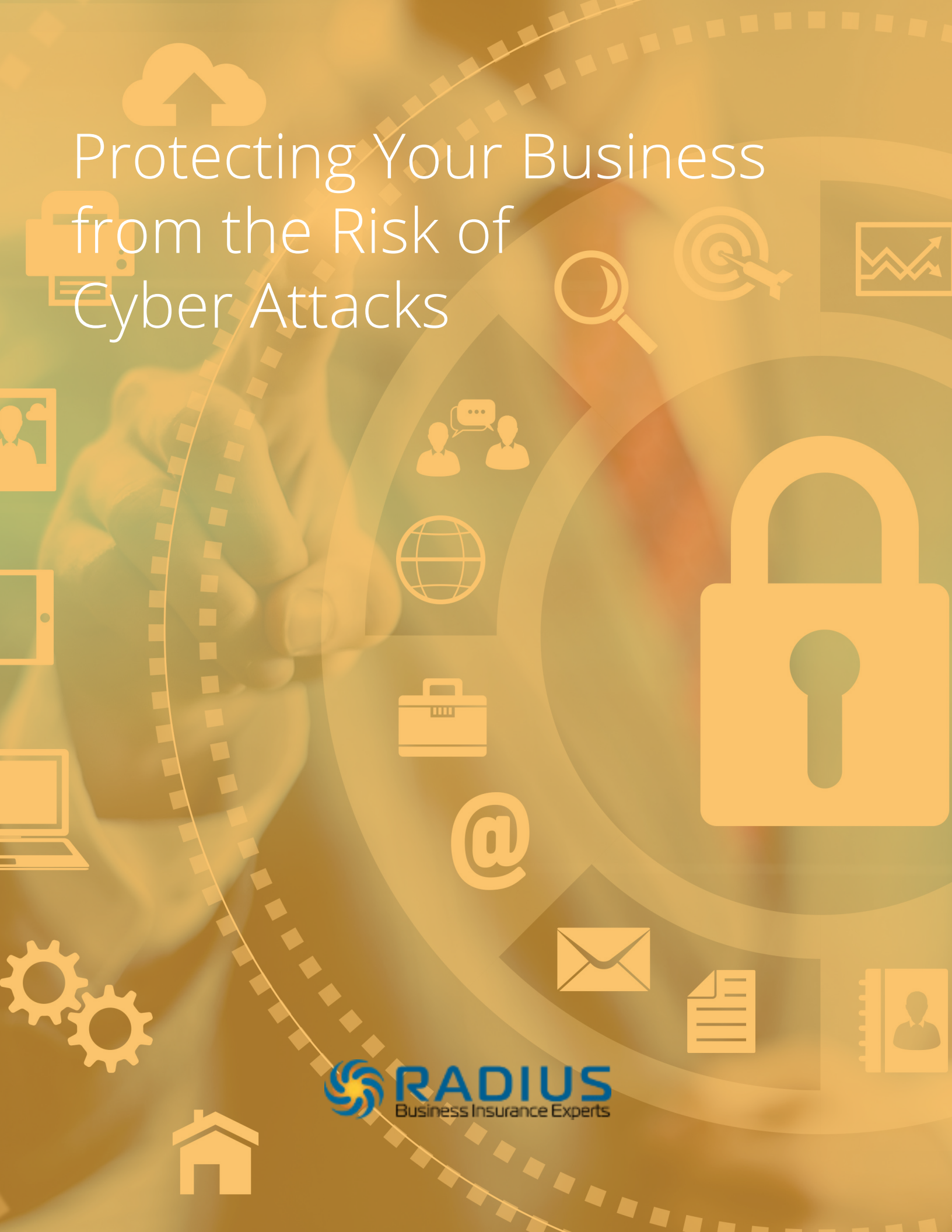
Protecting Your Business from the Risk of Cyber Attacks



RADIUS
Business Insurance Experts

Introduction

Businesses in 2017 face more threats than ever before. Traditional risks still exist, but for any business that works with sensitive data – whether industry specific or client-owned – cyber security is the fastest growing threat they face.

Moreover, most businesses aren't fully prepared. Even those with a strong IT plan to protect against breach and react if a problem occurs may not be protected through their insurance policies.

Risk assessment and management for cyber security threats is a relatively new addition to most insurance policies, and for many industries is not included in the Business Owner Policy (BOP) carried for general risk.

If you are one of those businesses that doesn't have a good plan in place for how to manage risk from cyber threats, it's important to evaluate your exposure, plan, and get the necessary insurance needed to transfer that risk in the event of an incursion.

In this guide, we're going to look at how to evaluate your current setup, what kind of impact an attack would have on your business, and how to build a plan that prevents and responds to cyber-attack should it happen.

Assessment

While any business is a potential target for cyber-attack, some are at greater risk than others. The more exposure you have in terms of data transfer, number of employees, accessibility to your technology hardware, and the sensitivity of the data you work with, the greater your risk of cyber-attack.

But that doesn't mean a company with relatively insignificant data isn't at risk. Much like theft and traditional crime, it only takes one person with a motive to create a potentially business-ending disaster if you're not prepared. So, it's vital that you spend some time identifying what could be at risk and how best to protect it.

Identifying Sensitive Information

Your company likely has a lot of information on hand – some of it highly sensitive data that could put your business at financial risk if it was compromised or stolen, and some of it...less so.

To ensure your IT efforts effectively protect your data against real threats you might face, it's important to identify which things fit the former category and which are more in the latter. What assets need protection and why?

This is going to be different for every company. A professional services firm that handles sensitive legal or financial data for clients has a much larger swath of sensitive information that needs to be protected than a restaurant. The most important thing to remember, however, is that every business has some sensitive data on hand. The difference is that, while most professional services firms are aware of their responsibility to assess and protect against their exposure to cyber-attack risk, the average small business is not.

And yet, financial accounts, payroll data, and other sensitive information is equally valuable to a small business, and if it is compromised, the results can be just as catastrophic.

The National Cyber Security Alliance and Symantec recently ran a study, finding that 66% of small businesses are dependent on the Internet for day to day operations, with 67% saying they have become more dependent in the year preceding the study.

In the same survey, nearly 70% of businesses surveyed handle some form of sensitive information that included customer data, financial records and reports, intellectual property, either owned or protected for a client.

And yet despite the high exposure to risk for so many companies, 77% stated they did not have a formal written Internet security policy for their employees. In fact, the statistics here are unnerving:

- 63% don't have social media policies for employees
- Only 60% have a privacy policy in place for how customer information is handled and only 52% have a plan in place for cyber security.
- Only 37% of businesses provide some form of training for employees to remain safe while using the Internet at work. The other two thirds? They allow the use of USB sticks and other potential hazards in the workplace.

The bottom line is that the average company isn't prepared for a cyber-attack, and whether you have payroll and financial records on hand that could damage you personally, or you are handling the intellectual property or financial data of a client, lack of preparation is a potentially hazardous situation for your business.

How Is Your IT Structure Currently Setup?

Your current setup is an important factor not only in assessing risk, but in preventing it. Proper IT management, including possibly bringing in an outside firm or MSP to support your efforts, is vital to ensuring things work in your favor.

To get started, ask yourself the following questions:

How is information stored?

Is your data stored locally on a secure server, in the cloud through a SaaS product, or do you have a third-party MSP that manages your data storage? Who has access and how easily it can be accessed remotely are important factors when assessing risk.

Who has access to data?

Who in your organization has access to data and when? While overprotecting data and locking out key employees can slow operations and harm productivity, open access without logging can make it impossible to track and protect against security breaches. A policy in place for access, nature of access, and handling of sensitive data is a must.

How do you protect data?

What resources are in place to protect your data? There are countless resources to protect your information, from firewalls to outside Internet access to VPNs for larger organizations, and data encryption for cloud stored data.

How are things being secured?

Who is on point when it comes to securing your data? Data security is not a one-time action. It requires constant, ongoing oversight by an IT professional to account for new threats. Do you have an IT professional on staff or do you work with a third-party MSP? Is anyone truly in charge of your data security?

How Is Your IT Structure Currently Setup?

It's hard to imagine the impact of something as abstract as a digital attack on your business. While an increasing number of businesses are facing the fallout from these attacks, studies show that very few understand what a cyber-attack really means and what would happen in the event of one.

Part of that is due to the varied nature of such attacks. From theft of sensitive data to a brute force attack designed to interrupt operations, there are several scenarios you need to be prepared for.

Data Theft – Data theft can happen in many ways. An employee downloading intellectual property to a USB stick and taking it home with them is data theft the same as a rogue hacker breaking into one of your servers. Both situations need to be accounted for in your plans.

Identify Theft – Every few months, a major corporation suffers a black eye in the press for data breaches that lose millions of user records, some including vital personal information. These are the big ones. Much smaller breaches occur every day as hackers steal personal information, financial records, or your own information, all potential tools for identity theft.

Server Attack – Data theft is terrifying, but what about a more basic attack against your businesses. DDOS attacks against servers can take down websites and interrupt operations for hours or even days if you're not ready. If you do business online, this is something that must be protected against.

Lost Devices – A lost laptop or company cellphone can contain large volumes of sensitive information. Be prepared with a lost device plan that can remotely remove this data or encrypt it to block access by third parties.

The cost of these attacks can vary dramatically. Downtime for your business has a static cost from lost productivity, emergency maintenance and repairs, and damage to your reputation. Then there are the more abstract costs, such as the impact of client information being stolen by a hacker.

From lost clients to potential lawsuits, the ramifications can be substantial, and without good protection, possibly even put your business at risk of failure.

Building a Cyber Security Plan

With the risks you face in mind, how do you go about creating a plan that will work to prevent these types of things from happening?

Because of technology and the rapid advance of new techniques both in security and bypassing security, it's impossible to 100% protect your business from these potential risks, but with the right mix of prevention and attentiveness, you can deter most attacks and be ready to respond if something does happen.

Cyber Attack Prevention

You can only transfer so much risk, so the first step is build a plan for prevention. This should include the following approaches to your cyber security situation:

- Evaluating your current structure to assess for security gaps. Looking for areas in which you are missing key protections or there are not existing policies.
- Creating relevant policies that protect your business including employee Internet use, data access, company device use, and data transfer protocols.
- Building procedures for how to onboard and handle the most sensitive information. This may include documentation to form a paper trail for anything you bring into the business.
- Assigning key stakeholders to oversee area of your cyber security. If you have an IT person on staff, they should be directly in charge of this with managerial oversight. If not, consider an MSP to support your efforts.

The goal with your prevention plan is to know exactly where you are weakest and act to prevent those weaknesses from being exploited.

Cyber Attack Resolution

If, despite your best efforts, there is an attack that impacts your business, how do you respond? A good cyber-attack resolution plan will address the fallout of an attack and what you do to recover, including:

- Your immediate response. What do you do when information is lost, servers are breached, or identity information is stolen? Who do you contact, how do you track down the cause of the attack, and what do you do to fix the vulnerability.

- Who is directly in charge of the situation when this happens? Your IT staff or MSP will be actively involved in addressing and resolving the situation, but who oversees determining why this happened and how to react to it in the future.

It's easy to patch it and forget it, thinking an attack is a fluke, especially if nothing particularly important was accessed. But if it happens once, it can happen again, so be ready to respond.

Cyber Attack Restitution

Finally, there is the fallout from a cyber-attack. No matter how well prepared you are and how fast you respond, there are negatives associated with having information stolen or impacted by an attack.

A good restitution plan will consider the impact that an attack or data breach might have on your customers or employees, and respond appropriately. That means:

- Immediate communication to anyone who is impacted with a clear overview of what happened and how you will respond.

- If your business is large enough, a PR plan for broader outreach, discussing the efforts your business is taking.

- A communications plan for describing what you will do and how you will do it to ensure such an attack won't happen again in the future.

The worst thing you can do when there is a cyber-attack is to ignore it or try to cover it up. Communicating with your attorney, reaching out to those affected, and executing a carefully prepared plan will all help ensure you minimize fallout from the situation.

Transferring Risk

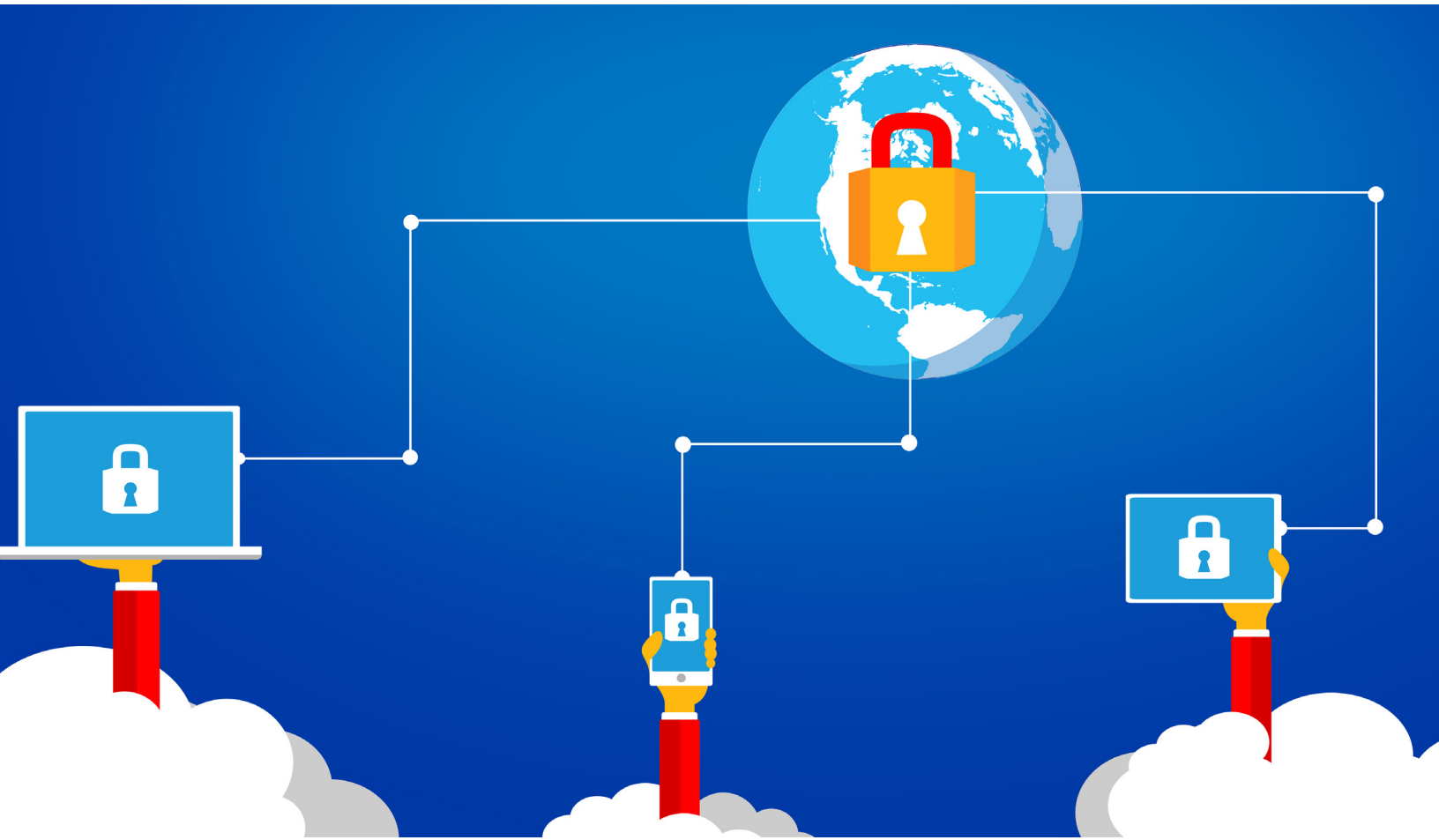
It's impossible to protect yourself 100% from a cyber-attack. The rising trend of digital crime in place of more traditional theft means businesses once safe from the risk of recurring crime and the high cost of security must make major changes.

Cyber security and IT are vital components of this, but so too is good insurance. But it's also important to understand the coverage options available to you in today's insurance market, and what you might already be covered for.

The Cyber Insurance Market

The market for cyber insurance has grown dramatically, from only a handful of carriers in the 90s to more than 50 major carriers offering plans with up to $300M in limits for businesses of all different types and sizes.

There are a lot of different things to consider in your own coverage, from the liability your company might hold as a third party holding customer information to the first party costs of lost business and reparations after an attack, so it's important to evaluate your options carefully and choose the insurance coverage that best fits your needs.



Cyber Insurance Coverage Options

There are several coverage options available depending on your business and current exposure to risk. Some of the most common include:

Security and privacy liability – This is one of the most important as it addresses the failure to keep third party information private and secure. This applies to failure of network security systems that might include breaches or transmission of a virus, and applies to personally identifiable information (PII), corporate confidential information (CCI), or protected health information (PHI).

Crisis management – After a cyber-attack or breach occurs, the cost of managing the ensuing fallout can be covered with a crisis management policy. This includes costs related to bad publicity, regulatory changes required and monitoring of parties affected (and the appropriate credit monitoring services).

Regulatory proceedings – If a privacy regulator such as the FTC, HIPAA or State Attorney General acts against your company after a breach, or if a fine is levied, this can provide some coverage, though certain fine coverage may be limited.

Data recovery – If data is lost or destroyed, the costs associated with recovering it, both in recreation of that data and restoration of it from backups or encrypted systems can be covered.

Cyber extortion – An increasingly common result of these attacks is extortion, through which a third party holds your systems or data hostage against payment. Some policies will cover portions of such costs depending on the situation.

The best way to ensure your business is properly protected against these risks is to speak with a broker who has specific experience working with insurers that protect against cyber risk.

By discussing your current exposure, the changes you plan on making to your security measures, and what can be done in addition to reduce those threats, you can ensure you have good protection against potential cyber security risks that supplements your BOP coverage.

Next Steps

The next step in the process is to sit down, evaluate the risks your business currently faces and plan of action for how to handle those risks.

Like any component of your business, there are several factors to consider, including:

- **Cost –** What is the cost of a breach for your business, and what can you do proactively to prevent it without incurring significant costs.
- **Resources –** What resources do you have in-house to address these issues now and will you need to pay for outside resources.
- **Productivity –** What impact will a breach have on employee productivity? What about the security measures put in place to protect against it.
- **Mitigation of Risk –** A careful balance of risk management through transfer and prevention is vital for cyber-attacks. Evaluation of each business individually is a must.
- **Scalability –** For growing businesses, your plans need to be scalable. This includes your IT directives, data management policies, and risk transfer choices.

But by evaluating how your business handles data, its exposure to risk and the potential cost of a cyber-attack, you be ready for whatever might happen, while getting the best possible coverage for your needs.

If you're ready to get started, Radius Insurance can help. We work with hundreds of insurance carriers that specialize in business insurance policies, including cyber coverage. We can help you evaluate your options and choose the best policy to fit your current risk exposure.

Call us today to learn more or to schedule a consultation to discuss how good cyber insurance can better protect your business.