

CYBERSECURITY:

Prepare, Plan
and Protect
Your Small Business

The impact that cyber risk can have on your business involves various interconnected factors, making them a challenge to understand and address comprehensively. Assessing your cyber risk and having a plan to protect your business in the event of a cyber-related incident is critical to your company's overall health and success.

While an essential step for all businesses, it is an even higher priority for those that operate in sectors where collecting personally identifiable information (PII) and personal health information (PHI) is essential to running the business, such as the healthcare, financial, and public sectors.

A quick overview of Personally Identifiable Information (PII)

PII is the most targeted type of information in a data breach. It includes any information used to help identify an individual and carries a privacy risk. Almost all businesses carry this type of information and are responsible for protecting it. It's critical to note that PII also lives in essential business documents, such as W-4s and I-9s.

Here are some of the most common examples of PII:

- Name
- Address
- Email
- Telephone number
- Date of birth
- Passport number
- Fingerprint
- Drivers license number
- Credit or debit card number
- Social Security number



A quick overview of Personal Health Information (PHI)

PHI is a record containing medical information.

Typically, this involves demographics, medical history, tests and lab results, mental health conditions, insurance information, and any other sensitive data that a healthcare provider might need to collect for patient care.

It's also important to note that PHI and PII breaches can carry different penalties, depending on how they're being used.

For example, the penalty structure for violating HIPAA laws can have more severe consequences, as penalties are determined by the Office for Civil Rights and are based on several "general factors" and the seriousness of the violation.

Meanwhile, PII breaches can be just as damaging but may depend on the nature of the exposed information, which will often include things like names and email addresses as opposed to highly sensitive health data.

On that note, not all PII is considered sensitive information.

In fact, some PII is available through the public domain. This information includes items that can be found within public records.



The consequences are costly

According to IBM's Cost of a Data Breach Report 2024, the global average cost of a data breach has risen to \$4.88 million, underscoring the growing financial impact of cyber incidents. Organizations also face substantial expenses related to investigation, containment, recovery, business disruption, regulatory response, and customer remediation. At the same time, ransomware continues to pose a significant threat. Recent industry data shows the average ransomware payment exceeds \$550,000, while even median payments commonly reach six figures. For many small businesses, a single cyber incident can threaten business continuity, making cybersecurity preparedness and cyber insurance critical components of risk management.

These are just some of the consequences that can result from a cybersecurity event affecting PII and PHI:

- Cost productivity
- Financial loss
- Brand reputation
- Customer loyalty
- Infrastructure and safety issues
- Business closure
- Government regulatory fines

Consider these items when creating a cybersecurity plan:

- Your industry
- Number of employees
- Hybrid working environments (and percentage of remote employees)
- Compliance and regulation mandates
- The type of data you collect and store
- Risk assessment
- Network visibility
- Employee training
- Cyber insurance policy

\$4.88M

Global average cost
of a data breach

\$2.2M

Average data breach
cost to an organization
for investigation and
recovery

\$554K

Median ransomware
demand amount



How can I keep my company safe from cyber attacks?

First, you must take a deep dive into your current cybersecurity posture.

Determine the calculation of the value of your sensitive information (in dollars!) and note the devices where that information resides and include all of this in your assessment.

Cybersecurity tools like SBAM's RiskAware Scanning Tool and SensCy Score Assessment can take the pain and take out the guesswork. Discover your unique cyber risks through an assessment and continuously scan and monitor the data across all your company's devices in real-time.

Second, you should implement cybersecurity best practices. Even if you're already doing this, it's good to regularly revisit this step continuously to ensure that all employees are actively following the company's security protocols.

- Be proactive and look for blind spots
- Deploy a network visibility security tool
- Don't forget to protect your cloud service(s)
- Ensure that all administrator accounts have multi-factor authentication (MFA)
- Educate and provide regular security awareness training for employees
- Request and review the cybersecurity posture assessments of subcontractors and vendors
- Run regular reports on the total dollar value of your cyber information
- Purchase a standalone cyber insurance policy; not a general liability policy with some cyber insurance baked in
- If you already have a cyber insurance policy, review it to ensure it's customized to your specific needs

Understanding cyber liability insurance

Cybersecurity best practices, including successful technology implementation, are closely linked to your company's ability to obtain and keep cyber insurance.

Are you already covered in the event of a cybersecurity event?

Cyber insurance is often excluded from general business insurance policies - and even when it is combined as part of a general policy, it contains many fine-print contingencies and is no replacement for cyber insurance that is tailored to a company's complex needs.

It's also important to note that there are different types of cyber insurance, namely, cyber liability insurance and data breach insurance.

Cyber liability insurance is ideal for larger businesses and typically covers a broader range of events, while data breach insurance may be a better, more affordable option for small businesses.

Data breach insurance typically covers immediate costs such as data recovery, legal fees, and your company's liability for a breach involving PHI and PII.

No matter which type you choose, keep in mind that cyber insurance policies only cover specific claims for your business. This means you'll still need other business policies for things like general liability, commercial property, and employment practices, among others.

Cyber insurance is not a luxury. It's a necessity that can keep your doors open in the aftermath of a cyber-related event.

One in three (33%) small businesses were hit by a ransomware attack. The average bill for rectifying a ransomware attack - considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, etc. - was \$1.85 million. But rectifying a ransomware attack doesn't mean you'll get your data back.

Only 65% of encrypted data was restored to businesses after ransoms were paid. If your stomach hurts after reading these numbers, you're not alone; damage like this can easily put a small to medium sized company out of business.

A cyber insurance policy can help mitigate these devastating and costly outcomes by limiting your cyber exposure and, in the event of a cyber incident, can also help absorb some of the associated costs.

However, there are steps you can take in the meantime to reduce your amount of cyber risk. By decreasing the volume of sensitive cyber information your business carries and knowing how prepared you are should a breach occur, you may be able to negotiate a more affordable cyber insurance policy - and it's just good cybersecurity practice.

This might include eliminating duplicate files, removing PII and PHI from employees' personal devices, and ensuring that all sensitive information is up to snuff with industry standards and regulations.

How do I get a cyber insurance policy?

Obtaining a new cyber insurance policy requires your business to meet specific criteria.

Insurance providers want proof that your company has cybersecurity accountability when applying for a new policy or renewing an existing one.

Unlike other insurance policies, cyber insurance coverage is typically negotiated based on several complex factors. These factors might include historical losses and claims, your company's risk profile, your industry, and your cybersecurity posture (the overall health of your business as it relates to security best practices).

Here are some additional factors to consider when shopping for a cyber insurance policy:

- You should expect to pay more if you work in a high-risk sector, including healthcare, public administration, technology, or finance.
- The more devices your company deploys, the higher your policy will likely be.
- Remote devices carry an even larger risk; so it's good to assess these on a regular basis.
- Your endpoint detection and response (EDR) software matters and is frequently a key component to obtaining a policy.
- Ensure that all employees are practicing basic cyber hygiene (have a plan in place and provide proof that it's working).
- Make multi-factor authentication (MFA) mandatory for all users, especially IT administrator accounts in software applications.

SBAM cybersecurity solutions for your small business

You need to prepare and protect your small business without spending a significant amount of money consulting with risk management companies that don't understand your specific needs.

SBAM provides a comprehensive experience by cutting through the noise and delivering the insights needed to assess your risk of a cyber breach, understand the volume and the dollar amount of your cyber information, and produce a strategic plan to protect your company.

Our three-step solution provides expert partners to help prepare and protect you from a cyber breach. We help you find the right service to fit your needs, so your business continues to run smoothly.

Each of our approved cyber partners will ensure that you:

1. Know the value of your sensitive information and where it lives on all your devices.
2. Have the training and plans in place to help lower your risk of a cyber-attack.
3. Obtain the right liability insurance coverage to help protect your company if a breach were to occur.

By utilizing our solutions, your small business will:

- Find the right-size cyber insurance policy coverage.
- Understand before and after cyber information value.
- Reduce financial risk via cyber hygiene practices.
- Support and plan a realistic, affordable cybersecurity preparedness and response plan.

Learn more at sbam.org/protect or call us at (800) 362-5461

Sources:

<https://riskassure.com/>

<https://senscy.com/>



Learn more at sbam.org/protect
or call us at (800) 362-5461

The information provided in this report is strictly for the convenience of our members and is for general informational purposes only. © 2024 Small Business Association of Michigan. All rights reserved.