2025 Guide to Cyber Insurance

for Small Businesses

RISKASSURE

Table of contents

01

What is cyber risk?

Nobody plans to close their business due to a cybersecurity event, yet it happens more than you might think. In fact, one in four small businesses are at risk of shutting down after a cyberattack.

The numbers don't lie: **Poorly managed cybersecurity can create lasting damage.** What once seemed like an issue reserved for enterprise-level corporations is now a pervasive battle impacting companies of all sizes at an increasingly alarming pace.

Nearly half of all cyberattacks target small businesses — and they're financially devastating. On average, it takes 241 days for an organization to identify and contain a data breach in 2025, according to the 2025 IBM Cost of a Data Breach report. And the global cost of cybercrime is expected to increase to $13.8 trillion by 2028.

Moreover, cyber incidents are on the rise and are expected to grow in volume and cost. Business leaders often reconsider entering into a partnership or agreement with another company or supplier if the organization did not have comprehensive cyber insurance.

Cyber risk can impact more than just the bottom line depending on your industry. Weaponized AI is ushering in a new era of threats, according to Harvard's Kennedy School. AI is increasingly used to identify and exploit security vulnerabilities in defense systems, corporate networks, and critical infrastructure. These attacks could potentially disable communications, manipulate satellite systems, or disrupt power grids.

Here are some other concerning numbers. Recent Microsoft Security research shows:

1 in 3

small businesses have experienced a cyber attack

81%

of small businesses say AI increases their need for additional security

$250,000

is the average cost to small businesses for a cyberattacks

Compounding an already devastating reality, CEOs bear the burden of these outcomes.

According to Thomson Reuters, **new SEC regulations hold CEOs and boards directly accountable for oversight and liability** related to security incidents. Incidents can quickly lead to physical harm, destruction of property, or environmental disasters.

Cyber risk is business risk

Company leaders must stop treating cybersecurity as a separate function of the business. Cyber risk touches every part of your organization. Financial, operational, and strategic risks are significant factors at play when running a successful business.

Cybersecurity is no exception and should be at the top of this list.

Think of it as a critical off-balance sheet item. Off-balance sheet items include contingent assets or liabilities such as unused commitments, letters of credit, and derivatives — things that are, unfortunately, often treated as afterthoughts.

As such, they're rarely — if ever — taken into consideration, let alone prioritized. But not prioritizing your cyber risk can have grave consequences.

To be blunt, the impact that cyber risk can have on your business is a complex, multi-layered issue, and it demands constant attention.

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's 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.

PII is the most targeted type of information in a data breach. But just how widespread is it? When assessing breaches by data type, IBM found that customer PII accounts for a staggering 53%.

A quick overview of PII

Personally identifiable information (PII) is 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
- Driver's license number
- Credit or debit card number
- Social Security number

A quick overview of PHI

Personal health information (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 the purposes of 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 a number of "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 actually available through the public domain. This information includes items that can be found within public records, such as phone books and online directories.

The consequences are costly

According to a 2025 IBM report, the global average cost of a data breach is $4.44M.

What's more **average breach costs in the U.S. reached a record $10 million**, a 9% increase over last year, driven in part by higher regulatory fines and detection and escalation costs. Yet, only 63% of respondents in the Travelers survey said they carry cyber insurance — only 54% of small businesses.

These are just some of the consequences that can result from a cybersecurity event:

- Lost productivity
- Financial loss
- Brand reputation
- Customer loyalty
- Infrastructure and safety issues
- Business closure

  Government regulatory fines

80%

of respondents say having cyber insurance is critical

Only 63%

of respondents said they carry cyber insurance

How can you mitigate the worst of these consequences?

Get strategic about your cybersecurity plan, and put a legitimate cybersecurity budget into play.

Get A Free Cyber Risk Information Assessment

Planning your cybersecurity budget

Small businesses may have a more challenging time allocating funds to a cybersecurity budget, but they must prioritize it.

At the time of this writing, nearly half of small businesses (47%) still need a dedicated cybersecurity budget, according to a study by Corvus. Here's another way of putting it: **nearly half of small businesses are prime targets for a cyberattack.**

While no simple feat, planning your cybersecurity budget doesn't have to become a massive research project. The actual amount companies spend on their security budget is often tied to the total IT spend. The total cybersecurity budget should be based on the company's size (number of employees), the IT infrastructure's complexity, and the volume of cyber information.

Budgets will vary from company to company, depending on several factors. According to the 2025 Ians Research Security Budget report, **the average organization dedicates nearly 11% of its IT budget to cybersecurity.**

Cybersecurity is a top-five business risk for most companies, but budgets aren’t growing at the same rate as the expanding scope of security responsibilities.

Exponential technology leaps are challenging existing cyber strategies. Meeting the moment requires renewed urgency and creativity.

Consider these items when planning or revisiting your cybersecurity budget:

- 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

02

How can I keep my company safe from cyberattacks?

First and foremost, 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.

Cyber information assessment tools like RiskAware can take the pain and the guesswork out of this step by continuously scanning and monitoring the data across all of your company's devices in real time.

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

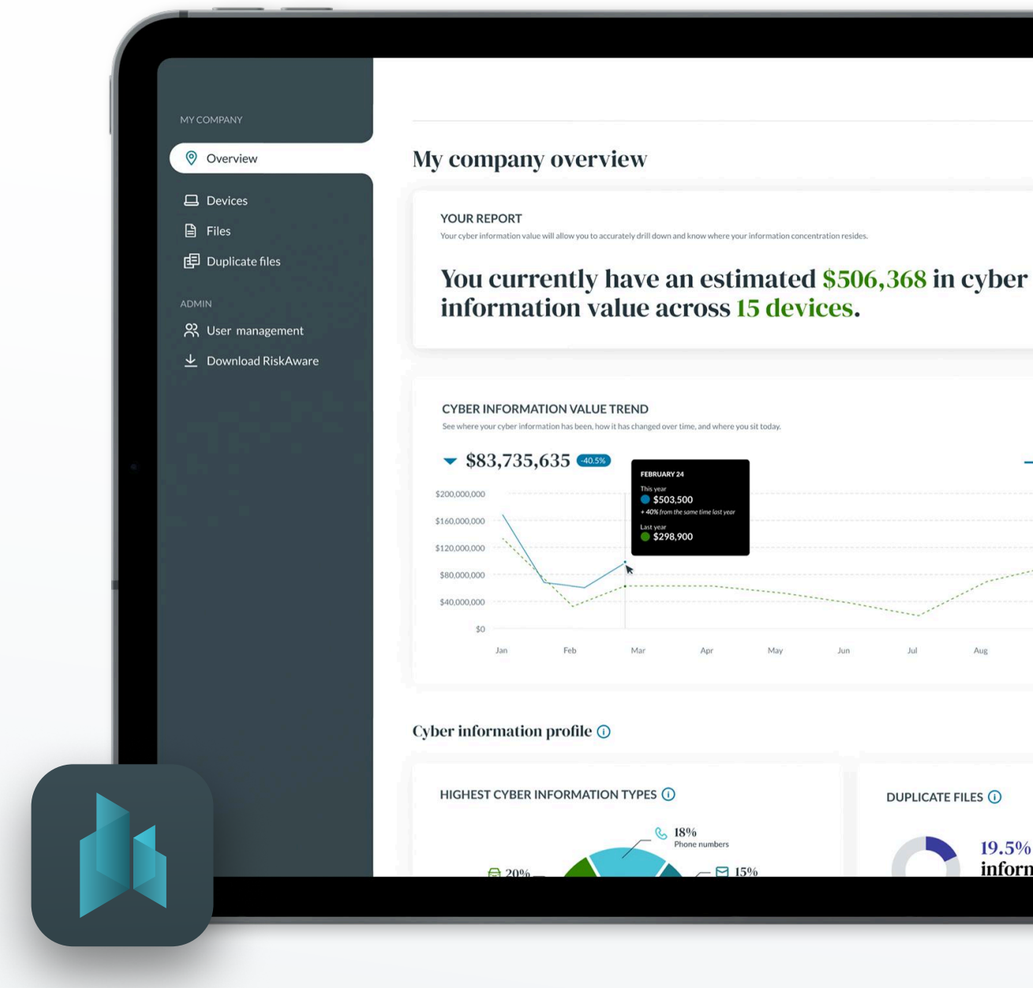
riskassure.com

These cybersecurity best practices should be non-negotiable:

- 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, right-size the one you currently have

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

Download RiskAware



Understanding cyber liability insurance

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

Unless you've already purchased a cyber-specific policy, the answer is no.

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.

Learn How To Right-Size Your Cyber Insurance Policy

Why does my business need cyber insurance?

59%

of SMBs were hit by a cyber attack in 2024

$2.73M

was the average cost to recover from a ransomware attack in 2025

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

A 2024 survey found that 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 $1.53 million.

But rectifying a ransomware attack doesn't mean you'll get your data back. Only 54% of encrypted data was restored to businesses after ransoms were paid in 2025. If your stomach hurts after reading these numbers, you're not alone; damage like this can easily take many small businesses to the cleaners.

Why does my business need cyber insurance?

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.

But cyber insurance isn't cheap, and it's essential to understand what you're paying for.

The upfront investment can be hard to swallow, especially for SMBs. Unlike larger firms which can more easily weather rate increases, if prices spike too dramatically (as they recently have), some smaller companies may not be able to afford coverage.

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, 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.

Learn How To Reduce My Cyber Risk

How much does it cost, and how do I get it?

Lately, the costs and coverage of cyber insurance are evolving as much as the cyber threat landscape itself.

According to Forrester research, premiums for cyber insurance will rise 15% as new AI threats emerge.

The widespread adoption of AI is likely to reverse the cyber market's recent deceleration. Implementing AI increases threat surface area and risk.

Business owners need to understand that the higher rates, while a direct response to an increasingly dangerous attack surface, don't always reflect the amount of money that insurers are willing to cover. This is why it's critical to gain visibility into the value of your cyber information.

When you can attach a total dollar amount to your company's sensitive data, you are more likely to get a cyber insurance policy based on your specific needs without paying for features or additional coverage that might not be applicable to your business.

Of course, the cost of cyber insurance policies will always vary based on your industry and your company's cyber information risk.

For example, health and finance businesses will find themselves with higher premiums due to the more sensitive nature of the data being collected.

Why are cyber insurance rates so high?

While the high cost of a cyber-related event plays a major factor in the price of cyber insurance, it's not the only reason behind premium spikes.

Cyber insurance carriers lack the critical visibility needed to accurately price policies. In recent years, carriers have also suffered significant loss ratios that could force many of them to abandon the market.

This has providers scrambling to find innovative solutions that will help combat bad actors, reduce cyberattacks, and make the cyber insurance market attractive enough to remain in it.

15%

rise in premiums in 2026 Forrester predicts as new AI threats and data demands emerge

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.

Learn How To Reduce My Cyber Risk

03

How can I measure the financial impact of my risk?

For small and middle market business owners, much more is at stake in terms of financial impact.

The Walmarts and the Amazons of the world aren't worried about going out of business over a breach; they're far more concerned with a hit to their bottom line. In most cases, these giant corporations have the means to recover after a financial blow.

Take AT&T as a prime example. **Nearly all of the company's customers' call and text records were exposed** in one of the most significant security events in recent history.

In 2024, 73 million customer records, including social security numbers were exposed. The breach, linked to malware that got into the system through through a third-party cloud data company, made global headlines, and instantly damaged the company's reputation.

While AT&T is still in business today, it hasn't yet completely recovered. The retailer was ordered to pay $177 million as part of its settlement.

If that number makes your stomach churn, consider the additional legal fees and other associated costs.

Take AT&T as a prime example:

73 million

customer records were compromised in a AT&T security event in 2024

$177 million

will be paid out as part of its settlement

A small business isn't dealing with the same volume of customers as AT&T, nor is it likely to house as much data.

Still, it's safe to say that a similar attack may force a smaller business to close its doors.

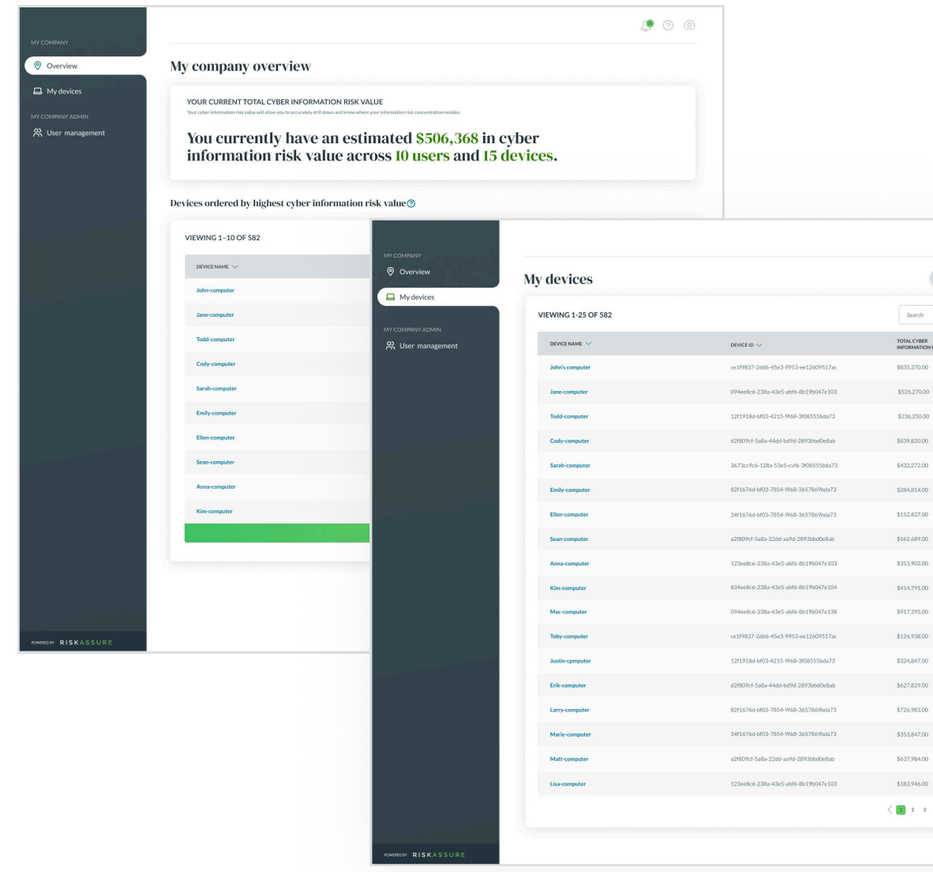
Understanding the financial value of your cyber risk

Every business carries a certain amount of cyber risk due to the sensitive information it stores across its network.

But knowing exactly how much that information is worth is like searching for the proverbial needle in the haystack.

That is unless you have an automated tool that can instantly and continuously monitor and calculate it for you.

Cue RiskAware



Think of RiskAware as a strategic partner that can help you deliver better outcomes for your business

As a small business owner, you need to manage the cost of your cyber insurance without spending a small fortune consulting with risk management companies that feed you jargon.

RiskAware provides a frictionless experience by cutting through the noise and delivering the insights needed to understand the volume and the dollar amount of your cyber information.

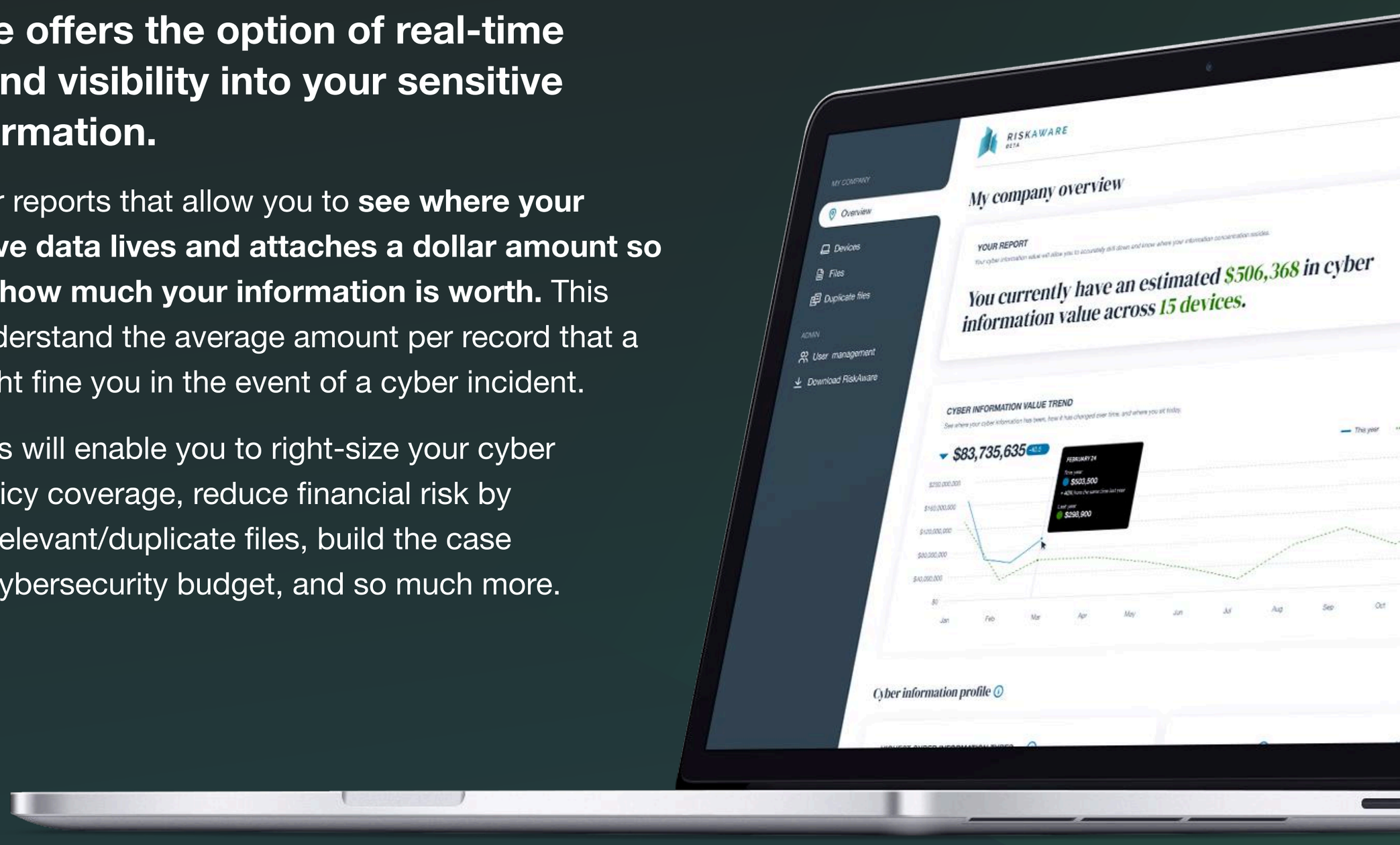
It also gives you visibility into your files and the devices where they reside, inspiring you to take action to reduce your risk.

How RiskAware works

RiskAware offers the option of real-time updates and visibility into your sensitive cyber information.

It runs regular reports that allow you to **see where your most sensitive data lives and attaches a dollar amount so you can see how much your information is worth.** This helps you understand the average amount per record that a regulator might fine you in the event of a cyber incident.

These insights will enable you to right-size your cyber insurance policy coverage, reduce financial risk by eliminating irrelevant/duplicate files, build the case for a robust cybersecurity budget, and so much more.



RiskAware empowers SMBs to:

01 **Right-size cyber insurance** policy coverage

02 Understand **"before and after"** cyber information value

03 Manage to an **acceptable baseline value**

04 **Reduce financial risk** via cyber hygiene practices

05 Support and **plan a realistic cybersecurity budget**

Learn More About RiskAware