EXTEND
RESOURCES

10 Steps for Developing a Smart Cyber Insurance Strategy

How to identify which risks to insure, evaluate suitable coverage, and minimize claims disputes

extendresources.com

Table of Contents

How has cyber insurance changed?

What does that mean for you?

Since ransomware became a reality and cyber insurance claims skyrocketed, insurance carriers have gained insight into the relationship between the quality of an insured's information security program management practices and the associated claims experience. As a result, carriers have:

- Set stronger risk management thresholds for obtaining policies,
- Increased premiums and deductibles,
- Limited coverage,
- Instituted select operational reporting requirements, and
- Continued to mandate communications protocols that must be followed in case of a covered breach.

Carriers' new insights and resulting changes have created significant impediments for those seeking the financial protection of a cyber insurance policy to protect against the broad spectrum of damages that can be inflicted on an organization due to an information security incident.

So, how can you effectively navigate the cyber insurance process to get the appropriate protection for your business, risk profile, and budget? Moreover, how can you reduce the likelihood of and effectively defend a claim dispute?

This guide outlines a high-level, stepwise approach to procuring and leveraging cost-effective cyber insurance aligned with your risk posture.

It starts with a comprehensive risk assessment.

Let's begin.

1. Carefully analyze the organization's information security risks.

Cybersecurity insurance is designed to protect organizations -- companies, institutions, and entities of all types -- from the financial risk of cybersecurity threats that cannot be reduced sufficiently using alternative methods. Before you explore cyber insurance options, you should understand what risks you need to insure, to what limits, and why.

Performing a risk assessment identifies vulnerabilities within an organization that could lead to security incidents and data breaches. When done correctly, this knowledge enables leadership and other stakeholders to prioritize resources, budget, and time to improve the organization's information security posture and enable it to better defend against cyberattacks.

Assessing risks also enables businesses to determine which risks may need to be mitigated using cyber insurance and identify appropriate coverage amounts. This front-end investment can bring significant returns to a company in terms of risk mitigation and creating a successful cyber insurance strategy.

Risk assessment is a systematic process that requires you to:

- Document your portfolio of assets, including in-house systems, processes, and people, as well as third parties that create, store, and manage your business' information,
- Understand and map the way those assets support your business operations,
- Determine ownership of the assets and who must address the related threats and vulnerabilities, and
- Recognize which assets can be used as an entry point or intrusion path to your data.

Assign a severity level to each risk using a scoring methodology that aligns with your business type, assets, processes, and security goals. The scores should be well defined so they are meaningful to stakeholders and can lead to better risk mitigation decisions.

When identifying risks, it can be helpful to consider the types of cyber threats your business could face. Cybercriminals target organizations differently depending on the various technologies they use or the industries, market segments, and geographies they represent.

Furthermore, a lack of security around your external attack surfaces (externally hosted assets, internet-based interactions, third-party vendors and service providers, etc.) can also make a company stand out as an easy target for hackers.

2. Rank risks from high to low based on criticality to the organization.

Now that you have identified and scored your risks based on the severity of the vulnerability and potential impact on your organization, you can determine which risks are most critical to resolve or mitigate to drive down inherent risk. This step helps you reduce the number of risks that may need to be covered by cyber insurance.

Special note: Lines of coverage available in the market today are designed to address a broad array of risks. Accordingly, if you reduce some but not all risks covered under a line of coverage, that coverage type may still be needed.

Business impact should play a role in ranking risks. Suppose a single asset supports multiple core business processes or is a prerequisite for other assets required to support your operation. In that case, the risks associated with that asset might rank higher than they would otherwise.

Rank the risks in priority order. Some organizations simply list them from high to low based on the risk score. Others use a risk priority matrix that combines other business- or security-specific criteria to differentiate levels of risk further. No matter the methodology you choose, this ranking exercise helps you make two valuable decisions.

Based on your budget, which risks can and are you willing to mitigate using information security controls and cyber defense strategies?

Which risks cannot currently be mitigated or have a residual risk that represents an ongoing financial exposure and should be included in your cyber insurance strategy?

Before shifting your focus to cyber insurance, consider leveraging the commonly used risk management approaches in section three to help decrease the risks you may want to insure.

3. Determine and implement the appropriate approach for managing each risk.

When you understand the nature of a risk, its potential impact on the organization, and its criticality compared to other risks, you have valuable information needed to make a well-informed risk management decision.

Before you explore cyber insurance options, exploring ways to reduce the inherent risk across your organization is beneficial.

When addressing risk, you have five options.

1

Avoid the risk through the discontinuation of an activity or the retirement of an asset.

For example, you may have multiple assets used to perform similar functions, such as three different project management tools used in various departments. To reduce risk, you can consolidate to a single project management software platform with one owner and retire the other two platforms.

2

Mitigate the risk through investment at whatever level the organization deems appropriate within a defined budget. This investment could include tools, training, policy and procedure development or modification, and other tactics. To the extent practicable, mitigate as many of the high-risk items as the budget will allow.

For example, many software platforms offer multi-factor authentication, but your policies may not require teams to leverage those security tools. Updating your policies and implementing a process to validate the use of MFA across your software assets can help you mitigate known risks. Or, if a critical vendor is ranked as a high risk, companies may consider shifting activities to an alternative vendor.

3

Transfer risk to third parties through leveraging contractual terms with third parties regarding security, indemnification, insurance requirements, and other provisions.

For example, when reviewing indemnification clauses for vendor contracts, consider what specific language would best protect you against losses arising from a data breach or cyberattack at or through one of your vendors. A thoughtful approach can help you transfer risk in the contracting process.

4

Accept the risk because the security incident risk level and the resulting impact on financial exposure and operations continuity are low.

For example, you may have an asset that's essentially an island, not connected to other networks, systems, or assets. If, following analysis, the risk of unauthorized access and deeper intrusion into a connected system or network is determined to be minimal, you may be willing to accept that risk.

5

Transfer any residual financial risk from risks you accepted or mitigated by procuring cybersecurity insurance for your organization.

The risk mitigation process enables you to set yourself up for effective management of a future data breach. When you can explain how you analyzed the information and why you logically took certain risk management steps, you can help protect your organization against liability exposure, such as litigation exposure, punitive damages, or regulatory fines.

Risk mitigation can also support your ability to complete carriers' required security questionnaires accurately. You will find more information on that topic in section six of this guide.

4. Once the decision is made to pursue risk transfer through insurance, determine which risks you want to insure and to what level of coverage.

At this stage, you've taken meaningful steps to avoid, mitigate, transfer risk through your contracting process, or accept the risks. You have one option to manage the residual financial risk: Transfer your exposure to an insurance carrier.

Based on your earlier assessment and scoring activities, you already understand the nature and severity of your remaining risks. To determine potential coverage amounts, you can use various market resources and reports to review average breach costs and typical claims amounts for different scenarios. Some resources classify information based on organization size, industry, and other factors. Insights from these resources can help you understand a potential range of exposure related to a particular type of breach.

Doing a little bit of homework and proactively arming yourself with this information can help you have more productive conversations with an insurance broker or carrier.

5. Identify and contact the carriers that provide the coverage you are seeking.

Most organizations use an insurance broker to quote and procure cyber insurance coverage from traditional carriers. This remains a logical option. A savvy broker with industry knowledge may know the latest breach cost statistics, which can help you validate your research. They can help you understand potential exposure, coverage options, and premiums.

Yet some brokers may not be well versed in cyber threats or cyber insurance policies and requirements. How do you find a broker who is skilled in this area? When interviewing potential candidates, ask a few key questions outlined below.

- What experience does the brokerage have in the cybersecurity insurance space?
- How long has the individual broker been writing cyber insurance policies?
- What changes have they seen (in requirements, coverage, etc.)?
- How do they judge whether an organization is insurable and to what level?
- How do they choose their carrier partners?

Today, there are also new players in the cyber insurance market. Designed to disrupt the traditional carrier offerings, these companies offer managed security operations services (such as monitoring and incident detection and response) bundled with insurance coverage. This type of service is designed to leverage insights from technical risk management activities to demonstrate cybersecurity maturity and drive down insurance premiums.

Investigating traditional and innovative insurance options may be helpful so you can determine what makes the most sense for your organization.

6. Complete the applications including the information security self-assessment questionnaires.

A self-assessment security questionnaire is your opportunity to demonstrate the quality of your security program to a prospective carrier.

You must answer the questions thoroughly and paint an accurate picture of your security practices. Not only do your answers help a carrier determine the level of risk your organization faces, but the carrier will hold you accountable for your answers in the event of a breach or claim for coverage. *That means you must maintain (or improve) your program and practices outlined in the questionnaire for the life of the policy or risk having a claims dispute if you experience an incident.*

Fortunately, you can now leverage your disciplined approach to risk assessment and mitigation. Doing that work in advance means you should be able to answer many risk questions easily and truthfully from the start.

Regarding questions about compliance, policies, and technical configurations, this is no time for DIY. Properly completing the questionnaire requires full knowledge of your security practices, policies, technologies, and systems. Working with a team of information security experts can help you deliver the detailed information carriers expect, resulting in sensible policy quotes that align with your unique environment and risk tolerance.

7. Receive and analyze quotes; determine which policy to pursue.

As traditional insurance carriers have gained knowledge about cyber threats and effective security management programs, the risks being insured in cyber insurance policies have become similar from carrier to carrier. Policies are commodity-oriented, and carriers compete for business.

However, there are various pricing "levers," such as coverage levels and the rating of the carrier, that your broker can fine-tune to meet your budget. You have some options if you are unsatisfied with the quotes provided.

Ask the broker to identify more carriers

Find out what universe of carriers they pursued for quotes. They may need to search a broader audience if they only selected two or three carriers. Or it might indicate they have limited relationships or expertise in this area. For the latter, you may want to choose a different broker.

Provide additional insights about your risk mitigation activities

The broker doesn't know about your security posture beyond the answers to the security questionnaire. When you can deliver additional insights about what you want to cover and why the risk likelihood is low, they can take that information to carriers for adjustments.

Organizations typically have some ability to influence underwriters on coverage parameters. You may even influence decisions around pricing based on the information you can provide from your risk assessment, mitigation activities, information security certifications, and the results of a third-party audit.

Special note: Like automotive insurance carriers that offer better rates when you agree to install a monitoring device in your vehicle, cyber insurance carriers are beginning to offer similar discounts. When an organization is willing to provide evidence of active threat monitoring and management, such as XDR or threat intelligence alert data, brokers and carriers may offer an opportunity for discounted policy premiums.

8. Review policy language to confirm it accurately describes the business process and associated risks.

Use this opportunity to compare the risk you want to cover to the details outlined in the policy. Scrutinize all the policy elements before making a decision and binding coverage.

- Which fundamental risks are being covered? Is anything missing?
- How does the proposed coverage align with the organization's risks as we perceive them?
- How are coverage determinations made, and how might our actions influence them?
- Does policy language map to how our organization operates?
- Will potential incidents we identified be covered? At what level?
- Are there limitations or other requirements we must be aware of?
- Are there additional riders we should consider for items not covered in the base policy?

As the potential policyholder, you have an opportunity to request alterations to the policy elements, coverage, and language with most companies. If you need a specific type of coverage or want to make sure certain elements are included, you can go back to the broker or carrier with that request.

9. Obtain the carrier's communication protocols insureds must follow should there be a covered incident.

Just as carriers hold you accountable for your answers on the security questionnaire, they will also hold you accountable to incident response communication protocols referenced in the policy. This important piece of knowledge can make the difference between avoiding or experiencing a claims dispute.

These protocols outline when and how to notify the carrier of a breach and the steps you must take throughout the incident response process. To fully leverage your cyber insurance policy, reduce the likelihood of claims disputes, and defend against them, it is critical that you follow the communication protocols exactly.

If your policy does not list the communication protocols, you must request them from the carrier. Then, practicing your incident response plan using those protocols is beneficial. The more you practice, the better the results you will experience during an actual data breach.

A special note about your incident response resources: The carrier will likely offer a cadre of incident response resources, such as attorneys, forensics specialists, PR advisors, etc., to you as part of its coverage offering. While this may be an attractive option, you are not obligated to use the carriers' preferred resources. If you have your own preferred incident response resources for performing those tasks, you may use them once they are approved by the carrier.

Be aware that you must *first* follow the carrier's protocols to notify them of your third-party resources and obtain the carrier's approval before engaging them. This is a relatively simple process, but failure to do so may result in a claims dispute.

10. Understand the carriers' expectations for reporting during the policy's life.

As cyber insurance policies evolve, so do carriers' reporting requirements. During the policy's life, a carrier may require you to provide updated information about your security program. Reporting requirements may include:

- Risk assessment and risk mitigation activities,
- Updated security questionnaires,
- Implementation of and reporting of specific data from security monitoring tools,
- Managed detection and response data, and
- Insights on your compliance with various information security frameworks and standards.

Beyond the current requirements, the market can expect ongoing enhancements to required reporting. In the future, carriers may take steps to evaluate further and validate the security practices to which the insured has attested on the security questionnaire.

Conclusion

The steps outlined in this guide aim to help you prepare to apply for, procure, and leverage the financial protections of a cyber insurance policy in a smart, cost-effective way.

Incorporating sound risk assessment and management principles into your cyber insurance strategy fosters your ability to access cost-effective coverage aligned with your risk tolerance. Beyond smart risk management practices, building awareness of cyber insurance limitations and requirements and aligning your policy with your security posture can help you reduce the likelihood of claims disputes when an incident occurs and position your organization to defend against potential breach-related liabilities.

The steps outlined in this guide require a disciplined approach to risk management and commitment from an organization's leadership. Leveraging a team with expertise in cyber insurance strategy can bring significant value to your organization and peace of mind to your stakeholders.

EXTEND
RESOURCES

Your Trusted Partner for Cyber Insurance Strategy

EXTEND's cyber insurance and managed information security services are designed to assist with every one of the steps outlined in this guide.

Our team brings the discipline, knowledge, and experience to assess risks holistically and create a well-reasoned treatment plan to support your efforts to procure cyber insurance.

Contact Us

203-479-9408

extendresources.com

info@extendresources.com

@thinkextend