



Cyber Insurance Is Changing: 5 Steps to Prepare

Cyber Insurance Is Increasingly Tied to Cybersecurity Maturity



Cyber Insurance is Becoming More Rigorous

Cyber insurance was once viewed as a relatively straightforward safety net: pay the premium, answer a few questions about your cybersecurity practices, and transfer some of the financial risk of a cyberattack to an insurer. That model is changing. As ransomware, business email compromise, data breaches, and other cyber incidents become more costly and sophisticated, insurers are taking a much closer look at how organizations actually manage cyber risk. Coverage requirements are becoming more specific, underwriting questions are becoming more technical, and businesses may find that having a policy is no longer enough.



For IT and business leaders, the message is clear: cyber insurance is increasingly tied to cybersecurity maturity.

What is changing:

1

COVERAGE

Requirements are becoming more specific.

2

UNDERWRITING

Questions are becoming more technical.

3

EXPECTATION

Having a policy may no longer be enough

Insurers are Assessing if Controls are Actually Working

The cyber insurance market has evolved significantly over the past several years. Insurers have learned from a growing volume of claims and are using that experience to better assess which organizations represent higher risk. That means insurers are asking more detailed questions about the controls organizations have in place and, increasingly, whether those controls are actually being used effectively.



What Insurers May Ask About

Depending on the insurer and policy, businesses may be asked about:

- | | | |
|--|---|--------------------------------------|
| 1 Multifactor authentication (MFA) | 2 Endpoint detection and response (EDR) | 3 Backup and disaster recovery |
| 4 Privileged access management | 5 Security awareness training | 6 Vulnerability and patch management |
| 7 Email security | 8 Network segmentation | 9 Incident response planning |
| 10 Security monitoring and threat detection | 11 Encryption and data protection | 12 Third-party risk management |
| 13 Business continuity and disaster recovery testing | | |



Checking the Box May Not Be Enough

The important distinction is that these are no longer simply technology questions. They are questions about risk management.

A company may have purchased an EDR platform, for example, but an insurer may want to know whether it covers all endpoints, whether alerts are monitored, how incidents are investigated, and whether you can demonstrate that the technology is functioning as intended.

THE QUESTION BEHIND THE QUESTION

Can you demonstrate that the control is functioning as intended?

That is the difference between owning security technology and demonstrating effective risk management.

The Application Itself Can Become a Risk

One of the biggest challenges for businesses is that cyber insurance applications can require detailed representations about their security environment. That creates an important responsibility for IT and business leaders: make sure the answers are accurate.

EXAMPLE: MFA REPRESENTATION

If an application states that MFA is enabled across the organization, but certain privileged accounts or remote-access systems are excluded, that discrepancy could become important following a claim.

USE THE APPLICATION AS A COMPARISON POINT

DOCUMENTED PRACTICE

What your policy application says is in place.

ACTUAL ENVIRONMENT

What is truly deployed, monitored, maintained, and used.

The Same Applies to Backups, Endpoint Protection, Vulnerability Management and Other Controls

Companies should therefore avoid treating the insurance application as an administrative exercise. It should be treated as an opportunity to compare their documented security practices with what is actually happening in the environment.

This is particularly important for growing businesses where IT environments have become more complex through:

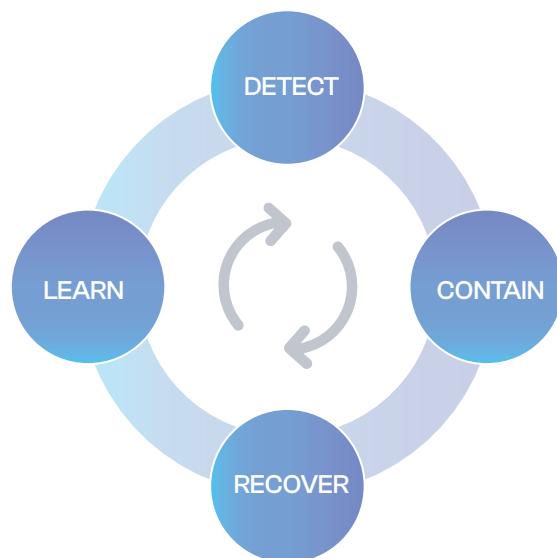
- + Cloud adoption
- + Remote work
- + Mergers & acquisitions
- + SaaS applications
- + Third-party integrations



Insurers Are Looking Beyond Technology

Another important shift is the growing emphasis on operational resilience. A business can have strong cybersecurity tools and still experience a major disruption if it doesn't know how to respond when something goes wrong.

Insurers increasingly want organizations to demonstrate that they can detect, contain, recover, from and learn from a cyber incident. That means businesses should have more than a collection of security products. They need documented processes and clearly assigned responsibilities.



More Than Security Products

Documented processes. Clear ownership. Practiced response.

A strong security stack cannot replace the ability to coordinate and recover when something goes wrong.

WHAT BUSINESSES SHOULD DO NOW

Understand Expectations. Identify Gaps Early.

Companies don't need to build an impenetrable security environment before purchasing cyber insurance. But you should understand what the insurer expects and identify gaps before those gaps become a problem.

HERE ARE FIVE PRACTICAL STEPS BUSINESSES CAN TAKE:

- 1 — Security Assessment
- 2 — Priority Controls
- 3 — Backup + Recovery
- 4 — Incident Response
- 5 — Policy Review

Steps 1-2: Assess First, Then Strengthen the Foundation

1

Treat the Insurance Application Like a Security Assessment

Don't wait until renewal time to discover that the organization can't confidently answer an insurer's questions. Review the current policy and application requirements with IT, security, finance, legal and executive leadership.

FOR EACH MAJOR CONTROL, DETERMINE:

- + What you currently have
- + If it's deployed everywhere it needs to be
- + Is it documented
- + Who owns it

This exercise can reveal security gaps that may otherwise go unnoticed.

2

Prioritize the Controls Insurers Care About Most

Focus first on foundational controls that reduce both cyber risk and potential insurance exposure. **These commonly include:**

MFA

Require strong authentication, particularly for remote access, cloud applications and privileged accounts.

Endpoint Protection

Deploy modern endpoint security and ensure alerts are actively monitored.

Patch Management

Establish a consistent process for identifying and remediating critical vulnerabilities.

Backups

Maintain secure, tested backups that are protected from ransomware and other attacks.

Security Awareness

Train employees to recognize phishing, socialengineering and other common attack techniques.

Incident Response

Establish a documented plan for responding to a cyber incident.

These controls are not simply about satisfying an insurer. They represent fundamental components of a modern cybersecurity practice.

Steps 3-5: Recover. Respond. Understand the Policy.

3

Test Your Backups and Your Recovery Plan

Having backups is not the same as being able to recover. Businesses should periodically test whether critical systems and data can actually be restored within an acceptable timeframe.

**TEST AGAINST SCENARIOS SUCH AS:**

- + Ransomware
- + Accidental deletion
- + Cloud service disruption
- + Compromised administrator accounts

A recovery plan that exists only on paper is unlikely to provide much comfort during a real incident.

4



Build and Exercise an Incident Response Plan

When a cyberattack occurs, the first few hours can have an enormous impact on the outcome. You should establish an incident response plan before an incident occurs and then practice it.

KEY CONTACTS SHOULD INCLUDE

IT • Security • Executive Leadership
Legal • Communications • HR
Other relevant functions

You should also understand your cyber insurance policy before an incident occurs.

5



Review Your Policy, Not Just Your Premium

Cyber insurance should be evaluated based on more than cost.

Business leaders should understand the scope of coverage, exclusions, deductibles or retentions, sublimits, ransomware provisions, business interruption coverage and requirements that must be satisfied to maintain coverage.

It's also important to understand how the policy interacts with the organization's actual cybersecurity practices. A lower premium isn't necessarily valuable if the organization doesn't understand what the policy cover what it requires.

THE BOTTOM LINE

Cyber Insurance Is Part of the Risk Strategy. It Is Not a Substitute for Cybersecurity.

Cyber insurance remains an important component of an organization's overall risk strategy. But it should not be viewed as a substitute for cybersecurity. The relationship is becoming increasingly interconnected:

BETTER SECURITY
can reduce cyber risk.

BETTER RISK MANAGEMENT
can improve insurability.

BETTER PREPARATION
can improve resilience
when an incident occurs.



USE RENEWAL AS A CYBERSECURITY CHECKPOINT

For business leaders, the most important step is to stop thinking about cyber insurance as an annual paperwork exercise. Instead, use the renewal process as a cybersecurity checkpoint.

Ask whether your company can confidently demonstrate that the controls reported to the insurer are actually deployed, monitored, tested and maintained.

And don't wait until renewal or worse, until after an incident to find out.