BITSIGHT

EBOOK

# How Bitsight Helps You Get Cyber Insurance Coverage

The state of cybersecurity feels volatile. Despite massive worldwide spending on risk management to the tune of $150 billion, cyber attacks keep happening. Ransomware attacks doubled in 2021, with average ransomware recovery costs doubling to $1.85 million and average downtime increasing to 22 days. Within the next few years, nearly half of companies worldwide will experience cyber attacks on their software supply chains. And, threats like malware and botnets (such as the recent Emotet re-emergence) are wreaking havoc worldwide.

As companies scramble to respond to exploding cyber incidents and a massive threat landscape, they're looking for cyber insurance coverage to protect themselves. According to a survey from Marsh McLennan and Microsoft, nearly a quarter of organizations say their spending on cyber insurance will rise by 25 percent or more in 2022.

But cyber insurers are responding to these industry challenges too. Many are rethinking their underwriting decisions altogether. The result? Stricter underwriting standards, tighter coverage expectations, increased premiums, and more denied applicants.

As companies look to gain or expand their cyber coverage and negotiate premiums, they need to effectively demonstrate their risk profile to insurers. By improving their cybersecurity strategy and showcasing the effectiveness of their program, companies have a better chance to get the right cyber insurance coverage at an ideal premium. In this ebook, we will explore:

**01** **A cyber insurer's strategy to underwriting policies**

**02** **The top 10 concerns that cyber insurers have**

**03** **How to strengthen your security posture to influence coverage**

## 1. A cyber insurer's strategy to underwriting policies

Before understanding how to influence your cyber insurance coverage, it's important to understand the mindset, processes, and strategy of a cyber insurer. Insurance companies are experiencing the same whiplash of the changing cybersecurity landscape just as much as the companies they insure. Insurers are paying out more and more for cyber attack claims, causing them to tighten expectations for coverage, deny applicants outside of their underwriting risk profile, and increase premiums.

Cyber insurance was originally intended to provide coverage in a similar method that traditional insurance, such as home and auto, is provided. This type of insurance covers events that likely won't happen, but could be very costly if they did. Consider that the average cost of recovering from a ransomware attack is $1.85 million. Organizations don't always have enough liquid assets on hand to recover from such a cost. That's why cyber insurance is so important; it transfers that risk to insurance. However with the explosion of ransomware, companies are suddenly faced with very costly, and much more likely incidents—which is making cyber insurance more expensive and harder to get.

Also consider that insurance is frequently cited as an important part of an overall cyber risk strategy to safeguard against the costs of a cyber attack. In 2021, there was a nearly 30 percent increase of companies purchasing some kind of cyber coverage. And in September 2021, 23 percent of Marsh McLennan's clients reduced their cyber limits, underscoring that cyber risk is growing.

With the need to cover high impact and high frequency events—and knowing that insurance is an integral component of a cyber risk strategy—it's no wonder that cyber insurers are responding in kind. Insurers aim to diversify their book of business, or the group of organizations they provide insurance coverage to, that pose different kinds and levels of risk. By having a variety of companies in their book, insurers mitigate the level of impact on their financials if an attack occurs since they are covering different types of risk. In this way, they can offer valuable policies that pay claims, but are careful to avoid large exposure levels with broad policy coverage.

### Cyber Insurance Terms

| Who | Definition |
|---|---|
| **Applicant** | Organization that is applying for cyber insurance coverage |
| **Book of Business** | The group of organizations that an insurance company will provide coverage to |
| **Broker** | Individual who represents an applicant who is seeking coverage and helps to place them with an insurer |
| **Insured** | Organization that has received cyber insurance coverage |
| **Insurer or Carrier** | Provides insurance coverage by evaluating an applicant's risk profile against their risk appetite and determines the premium level in exchange for coverage |
| **Underwriter** | The party responsible for assessing how much risk the insurer will take on as part of the insurance process |

To be eligible for coverage, underwriters have to determine how applicants are preventing claims. They do this as part of the insurance application process. This process includes an in-depth evaluation of an applicant's cyber risk posture to determine how to underwrite a policy. The application process can generally be described in five steps:

1. The applicant or their broker decides which insurers to seek coverage from
2. The applicant and/or broker fills out the coverage application provided by the insurer
3. The underwriter from the insurer collects data to put together the applicant's risk profile
4. The underwriter reviews the applicant's risk profile against the insurer's underwriting guidelines
5. The underwriter decides to either approve and set a premium in exchange for coverage, or deny coverage

Step 3 is the most critical place for applicants to focus on. Applications have to meet the insurer's risk appetite based on the insurer's proprietary underwriting systems. These systems are made up of a variety of factors, including:

- The state of the cyber market
- Anticipated risk and likelihood of attacks
- Historical claims data
- Overall risk and diversification of  their book of business

> "Insurance companies are experiencing the same whiplash of the changing cybersecurity landscape just as much as the companies they insure.

We've already covered the state of the cyber market in depth, but to reiterate: the rocketing growth of cyber attacks means there is more risk than ever in the cyber market. There is a constant and unrelenting risk of a cyber attack on any size company anywhere in the world. Insurers need to assume that any applicant is at risk of a cyber incident; it's a question of how resilient the applicant is to withstand or quickly recover from cyber events. This question leads us to the next section: data an insurer will consider when building an applicant's risk profile.

## 2. The top 10 concerns that cyber insurers have

No organization is immune from determined cyber criminals. But, there are best practices for minimizing the likelihood of becoming a victim. Chief among them is a relentless focus on cyber hygiene—the practice of ensuring that the organization is performing effectively every day. An applicant's overall cyber health sets the foundation for their risk profile and likelihood to get the right cyber insurance coverage. Good cyber hygiene significantly lowers the chance of cyber incidents; therefore, an insurer will thoroughly evaluate it.

At its core, cyber hygiene is a set of essential practices and tasks a company uses to keep systems, data, and users secure. With this in mind, insurers have top concerns that point to an applicant's overall cyber health, posture, resiliency, and maturity to make their underwriting decisions. From an insurer's perspective, knowing if a company can effectively address these concerns is a good way to start understanding their cyber hygiene. These concerns are:

1. **Access control**
2. **Insecure open ports**
3. **Patch, vulnerability, and configuration management**
4. **Email and web filtering**
5. **Endpoint detection and response (EDR) and malware protection**
6. **Cybersecurity awareness training and phishing testing**
7. **Incident response planning, logging, and monitoring**
8. **Supply chain security**
9. **Secure and tested backups**
10. **Overall cybersecurity hygiene**

A strong candidate for cyber insurance is an organization that has processes in place to address these concerns, which shows a level of high cyber hygiene and maturity. In fact, it may be a minimum requirement to adopt certain controls for them. Not only does evaluating these concerns give insurers an unbiased view of an applicant's cybersecurity program, it helps them verify the accuracy of the information they receive from an applicant during the coverage application process.

Insurers use a variety of solutions to help them understand an applicant's cyber performance, such as a cybersecurity rating. In fact, half of all global cyber insurance premiums are underwritten by Bitsight users who leverage an applicant's Bitsight Rating as one way to understand their cyber hygiene. Think of the Bitsight Security Rating like a credit rating—if someone missed a payment by the due date, their credit score might be impacted and then need time to recover.

“

In fact, half of all global cyber insurance premiums are underwritten by Bitsight users who leverage an applicant's Bitsight Rating as one way to understand their cyber hygiene.

When it comes to cyber insurance, applicants need to maintain strong cybersecurity throughout the policy period. Without that incentive, some applicants might treat cybersecurity as a once-a-year exercise, leaving insurers vulnerable throughout the policy period.

Because the Bitsight Rating operates like a credit rating—taking into account past and current performance as well as continuous improvements—underwriters trust it as a resource to:

- Evaluate risk profile within underwriting decisions
- Evaluate potential security threats through loss control programs
- Manage aggregate risk and data trends through portfolio management

> “
>
> Although Bitsight cannot influence the risk appetite of an insurance company, we can help you understand your cyber hygiene while proving to insurers that you are invested in your security posture, which does influence the coverage decision.

## 3. Strengthen security posture & influence insurance coverage

With this in mind, applicants need to be prepared to explain their cyber posture and processes in depth. A strong cybersecurity program helps insurers infer that an applicant isn't simply transferring cyber risk to their carrier in lieu of effective security controls. The best candidate for cyber insurance will demonstrate that they have processes in place to identify cyber risk, mitigate threats, monitor their security program for effectiveness, and improve over time.

This is where Bitsight can help applicants influence their cyber coverage. By showcasing the effectiveness of their cybersecurity programs, applicants can provide a full picture of their risk profile to insurers. Bitsight enables applicants to understand:

- Their risk profile
- Areas that need remediation
- How to prioritize those remediation areas
- Compromised systems
- 3hird- and fourth-party partners that may be compromised

Bitsight helps companies strengthen their application or obtain a better premium through improving cybersecurity posture and remediating vulnerabilities. Although Bitsight cannot influence the risk appetite of an insurance company, we can help you understand your cyber hygiene while proving to insurers that you are invested in your security posture, which does influence the coverage decision.

## Understanding & improving cyber hygiene with Security Performance Management

According to a recent study by Marsh McLennan, 37 percent of companies rate their cyber hygiene as satisfactory or better, while 40 percent say it needs improvement. Bitsight Security Performance Management (SPM) empowers companies to regularly assess and improve their cybersecurity hygiene to enhance their overall posture. As a result, SPM helps companies put themselves into the best position possible for insurance applications and negotiating premiums.

SPM supports evidence-based cyber risk monitoring, enabling applicants to set and work towards performance targets as well as communicate progress. For example, companies can gain insight into how effective their regular processes (such as patching cadence or control implementation) are and how they impact their cybersecurity posture.

A fundamental tenet of SPM is the ability to see an organization's cybersecurity performance over time, which ultimately guides the organization's decisions. This is especially important for cyber insurers as they look at a company's overall cyber health. If insurers can see improvements over time, or continuously strong cyber health, they can infer that there is a lower risk of successful ransomware and other cyber attacks, which boosts an applicant's chances at gaining coverage and improving premiums.

## Validate your coverage with Financial Quantification for Enterprise Cyber Risk

Companies that already have cyber insurance coverage may be wondering whether they should increase or decrease their limits. Although the knee-jerk reaction to cyber incidents and ransomware threats may be to seek more coverage, it may not be necessary based on what is at risk in your organization.

Bitsight's Financial Quantification for Enterprise Cyber Risk helps companies assess their financial exposure to cyber risk so they can calibrate their insurance coverage. Financial Quantification translates cyber risk into financial terms so companies can immediately understand the costs associated with a breach. This universal language around cyber risk puts their cybersecurity posture into an easily understandable context. By quickly understanding the likelihood and impact of a cyber attack in financial terms, companies can validate their premiums and coverage. And, the solution consists of proven models developed for cyber insurance and enterprise risk management.

Financial Quantification recently enabled Fordham University to successfully argue for lower insurance rates. According to CISO Jason Benedict, "The carriers were inferring that we presented more risk than we actually do based on a minimalistic assessment document and were quoting increased premiums. However, with Bitsight we were able to use real data to bring about a favorable negotiation."

Bitsight helps companies position themselves for cyber insurance applications and negotiating premiums. Companies around the world use Bitsight to strengthen their security posture, illustrate program effectiveness over time, and improve every day. If you're ready to learn more, visit **bitsight.com/security-performance-management**

Bitsight is a cyber risk management leader transforming how companies manage exposure, performance, and risk for themselves and their third parties. Companies rely on Bitsight to prioritize their cybersecurity investments, build greater trust within their ecosystem, and reduce their chances of financial loss. Built on over a decade of technological innovation, its integrated solutions deliver value across enterprise security performance, digital supply chains, cyber insurance, and data analysis.

BOSTON (HQ) RALEIGH NEW YORK LISBON SINGAPORE BUENOS AIRES

BITSIGHT