Blumira

FIFTHWALL SOLUTIONS

THE CURRENT STATE OF CYBER INSURANCE

THE CURRENT STATE OF CYBER INSURANCE

The cyber insurance industry is undergoing a massive shift. Rising premiums, changing requirements and a lack of consistency across the industry creates challenges for organizations that need coverage.

Now is the time to get clarity on how cyber insurance will change, and what security controls are needed to stay ahead of those changes. For managed service providers (MSPs), this is critical not just for their own business, but for their clients as well

The Evolution of Cyber Insurance

Over the past decade, the cyber insurance industry has operated much like the wild west, in which over-eager underwriters wrote policies without fully understanding their risk — or in some cases even understanding cybersecurity at all.

However, with the rise of ransomware and business email compromise (BEC), many insurance providers are taking on bigger losses than they had initially anticipated.

To right the ship, insurers are looking at three main options:

- Cut bait and leave the industry altogether, accepting their losses
- Dramatically raise premiums while lowering coverage limits
- Mandate better cybersecurity standards based on incident and breach data they've acquired

For some, it's already happening with premiums doubling or tripling and has created confusion and frustration for companies looking to renew or acquire cyber insurance.

What is Cybersecurity Insurance?

Cyber liability insurance is a type of insurance that provides protection against risks related to losses involving a company's digital assets. This could include irreversible damage or loss of company data due to ransomware, loss of time or productivity due to an attacker damaging network infrastructure, or loss or breach of customer data.

THE FUTURE OF CYBER INSURANCE

There's no question that the cyber insurance industry will tighten and become more standardized — it's just a matter of when. Cyber insurance providers that remain in the market have already begun to enforce more stringent cybersecurity requirements; by only providing coverage for companies with certain security controls, providers believe they can mitigate losses.

As cyber insurers gather more data about why breaches happen, they will use that data to better inform their policies and requirements. In the future, cyber insurance providers will continue to require critical controls that prevent breaches — or they will provide incentives in the form of significant discounts. Security information and event management (SIEM) can significantly reduce the risk of a cyberattack, for example, so insurers may give discounts to organizations that have implemented a SIEM, which can even potentially offset the cost of the SIEM altogether.

The lack of regulation in the cyber insurance industry has created issues around clients misrepresenting their infrastructure. Travelers Insurance recently filed a lawsuit claiming that its client that experienced a ransomware attack misrepresented their use of MFA. Issues such as these will likely encourage insurance companies to look more closely at their customers' tech stack.

Just as auto insurers place beacons on customers' cars to understand their driving habits, cyber insurance providers may enforce requirements by developing a better understanding of their customers' environments. For example, some insurers have already started to run external scans on their clients' networks.

Organizations with a cyber insurance policy, or considering a policy, should get in front of these changing requirements. By implementing these now, they can avoid expensive, low-quality, last-minute implementations when an insurance renewal is due. Usually renewals come on short notice and delivering a quality implementation of new security controls is not possible in those timelines.

WHO NEEDS CYBER INSURANCE?

Cyber liability insurance typically provides financial resources for digital forensics experts, legal experts, and other specialized resources that can help identify how the attack occurred, what the extent of the incident was, and what legal obligations arise from the incident.

A company would want cyber insurance to protect against the financial costs of an incident that impacts their digital assets. The costs of a cyber incident can be very high. According to Palo Alto, the average ransomware payment was **$925,162** in the first five months of 2022, which was **71%** higher than last year's average.

The cost of a breach can be even higher, which includes legal fees, penalties, and other costs to remediate or minimize the impact to customers. The average cost of a breach in 2021 was **$4.24 million**, according to IBM's report — the highest average total throughout the report's **17-year** history.

The financial impact of a ransomware attack or breach is even more devastating for small and midsize businesses (SMBs) that often don't have the budget or resources to successfully recover from an incident. Over **40%** of cyberattacks target SMBs; but **75%** of SMBs report that they don't have the personnel to address IT security.

WHY AN MSP NEEDS CYBER INSURANCE

An MSP would want cyber liability insurance to protect their own business from cyberattacks. However, an MSP's insurance needs to go beyond cyber liability insurance. An MSP's actions could potentially create a situation where one of their customers experiences a cyber incident, which may not be covered under an MSP's cyber liability insurance. Or a threat actor could use an MSP's remote management and monitoring (RMM) software to run a ransomware attack against their clients. An MSP should consider the benefits of Tech Errors & Omissions insurance, which would provide protection against mistakes that may result in a loss to a customer.

An MSP should also encourage their customers to obtain cyber liability insurance. Some MSPs have been shifting to a model where they would only offer support contracts to customers with cyber liability insurance. The MSP benefits from insured customers, because the customer is more likely to adopt a proactive approach to cybersecurity controls.

Insured customers would also have access to better specialized IT resources in the event of an incident, which can prevent the MSP from being overworked — especially in the event of a widespread incident that may impact multiple customers in a short period of time. Cyber insurance may also provide reimbursement to an MSP for emergency or after-hours labor required to recover from an incident.

GETTING CYBER INSURANCE

In the past, the price of cyber liability insurance was based on the size of the policy, the size of the insured company, and the company's risk factors. Insurance vendors would typically provide a survey of questions relating to a company's technology infrastructure, and would use those items to determine risk.

Today, insurers have specific security controls that are a must-have. These sometimes are required directly via documents that lay out the must-have controls. In other cases, the insurer will price the policy prohibitively high if organizations don't have the required security controls in place.

For example, they may not directly require MFA, but they may triple the price of the policy if MFA is not in place to protect access to high-risk systems. Year over year, renewals of the same policy tend to have more strict requirements in order to qualify for renewal.

Top Security Controls For Cyber Insurance

Some of the most common security controls that insurers ask for include:

Endpoint detection and response (EDR). An EDR solution continuously monitors endpoints to detect malicious behavior. It's often a requirement for cyber insurance because it enables organizations to proactively and reactively hunt for indicators of compromise (IoCs).

Next-generation antivirus (NGAV). While traditional antivirus solely relies on signature-based detection, NGAV uses modern techniques such as AI and behavioral-based detection to block threats.

End-user training. Employee training is becoming increasingly important to insurers, especially because phishing is one of the most common ways an attacker infiltrates an environment.

Segregated backups. Backups are crucial for ransomware recovery, since it can be an indicator of whether or not a company can recover quickly from the event. However, backups that are separate from where the information is initially stored is even better. Many cyber insurers also require encrypted backups to ensure the integrity of the data remains intact.

Security information and event management (SIEM). A SIEM collects and converges data from different parts of an IT environment for the intent of security monitoring. This helps an organization — and an insurance company — determine what happened (and when) in the event of an attack. Today's SIEMs commonly have detection and response capabilities, making the solution even more valuable for proactive protection.

These controls are not just important for cyber insurance, but they can also help to meet compliance requirements and improve your overall security maturity.

WHAT'S COVERED?

Each policy varies, so it's important to contact your specific provider to determine exactly what is covered by your insurer. Insurance agents who routinely write cyber liability policies are experienced in helping their customers determine an appropriate level of coverage.

Some policies may not cover legal or forensics costs, and some may have limits on how much of these services would be covered. The legal and forensics costs can be very high, and some companies find that those costs eat away at a significant portion of the policy, leaving little for things like possible ransom payments.

It is very important that you understand the costs of a cyber incident, especially if you would consider paying a ransom using an insurance policy.

The Big What-If: Ransomware

Most cyber insurance policies cover ransomware incidents. However, some providers require their customers to fill out separate applications with more stringent requirements to acquire more coverage that would cover ransomware. Policies will also typically specify coverage for double extortion ransom, or when a threat actor exfiltrates a victim's data in addition to encrypting it and threatens to leak that data unless a ransom is paid. For these reasons, it's crucial that organizations discuss their specific coverage with their provider.

Insurance policies may have a limit based on the total ransomware coverage. So, for example, if a total ransomware coverage limit is $1 million and the ransom is $1 million, then an insurance provider will not pay anything except for the initial ransom payment.

It's important to consider that the total cost of a ransomware incident often stretches beyond the cost of the initial ransom; it can include legal fees, forensic experts, potential penalties and fines, remediation costs, and more.

Organizations should understand a policy's specific coverage details before entering into an agreement with an insurance provider or renewing a contract.

WHAT TO EXPECT:
THE CYBER INSURANCE CLAIMS PROCESS

What happens when you experience a suspected incident, and you carry cyber liability insurance? Each policy varies, but here's a general idea of what you can expect when working with a cyber insurance company

STEP 1 Contacting Your Agent

First off, your internal resource who manages your insurance policies should contact your insurance agent, and notify them that you suspect that a cyber incident has occured. Some carriers now have dedicated contact methods as well for this purpose.

STEP 2 Legal Team Steps In

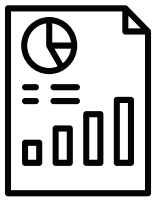
Once insurance is engaged, they will typically assign a specialized legal team to help protect your company. The legal team may engage with one or more vendors to perform a thorough investigation to determine the nature and extent of the suspected incident. It is important to note that everything is still suspected at this phase. In the eyes of the insurer and legal team, a breach needs to be investigated before it is confirmed.

During this time, the legal team will start to advise you on next steps, including internal and external communication. Inadvertent disclosures of your suspected incident at this time can cause complications as the legal team works to minimize your exposure to the various impacts of a breach or other similar incident.

Forensic Investigation

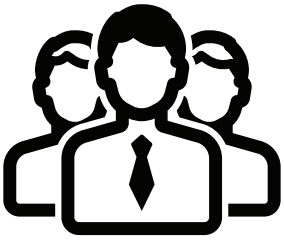
STEP 3

The legal team will engage a forensics team to work with your internal or outsourced IT team and get the necessary level of access to systems and data, which they will use to confirm a suspected incident, and determine its exact nature of the incident. If an incident is confirmed, and there was access or theft of data, a specialized firm may need to perform data analysis to categorize the accessed/stolen data according to various regulated categories, such as health data, employee data, financial data, and less commonly, forms of classified data.



STEP 4 **Incident Report**

Next, the legal team, in conjunction with other parties, will use the forensic and data analysis to prepare an incident report. This would take the form of a formal document that lays out the timeline of the incident, suspected or confirmed attacker techniques that were used to gain access to your systems, and what actions the attacker took during the attack.



Get Help With Incident Disclosure

STEP 5

The legal team will then use all this information to tell you what you are required to to disclose from a legal and regulatory perspective. In some cases, you must notify only those individuals who were impacted. In other cases, you are required to make public disclosure, and/or disclosures to government agencies.

The legal team will assist you in only taking required actions, and going no further beyond that point. Your specific policy may also have allowances for costs you may incur for notification, and in some cases offering free credit monitoring to impacted individuals.

LOGGING, RETENTION AND THREAT DETECTION: THE THREE MUSKETEERS OF CYBER INSURANCE

Logging

A SIEM provides a very accurate picture of how an attacker entered systems, when they first entered, what systems the attacker touched, and what data they accessed. This is important to the insurer because they want to be able to limit the scope of the response as much as possible to reduce their overall costs.

In some cases, the legal obligations following a data breach depend on the number of people, customers, or records breached. Without comprehensive logs available, the insurer may need to assume that the entire network is breached, and undergo much more expensive forensics and legal services in response.

Lack of sufficient logging may also lead to an expensive or complicated public relations issue for the company.

Data Retention

The numbers vary based on different reports, but it is common for an attacker to linger in a network for weeks or months before conducting damaging attacks against data or systems.

Like with logging, an insurance company wants to know as much information as possible about an incident. When an organization retains data for at least 90 days — or even better, six months to a year — an insurance provider can determine how long an attacker was in an environment. Data retention also expedites the recovery and restoration process after a breach or ransomware incident, helping with business continuity.

In addition to being long-term, log retention should also be immutable, meaning that they cannot be changed or deleted. This is important because attackers commonly clear logs to hide their tracks. Organizations should store logs outside of their own environment to prevent attackers from doing this.

Threat Detection

Insurers want to limit the impact of an attack as much as possible, and one way that this can be limited is by detecting an attacker early, before they have a chance to damage or exfiltrate data.

Having effective threat detection can greatly limit an insurer's financial obligations if an attacker can be eliminated from the network within hours of their initial entry. Breaches that took more than 200 days to identify and contain resulted in 35% higher cost for organizations, at $4.8 million on average, according to IBM's Cost of a Data Breach report.

Without early detection, organizations can suffer from longer breach lifecycles, resulting in a negative impact to their bottom line and therefore an insurer's bottom line, making a provider less likely to provide comprehensive coverage.

HOW BLUMIRA CAN HELP

Blumira can help organizations of any industry meet log monitoring, audit trail, data retention, detection and response requirements for cybersecurity insurance policies and other compliance regulations, such as HIPAA, PCI DSS, FFIEC, NIST, CMMC and more.

Blumira's cloud SIEM+XDR is a good fit for many companies that want to improve their security posture while qualifying for cost-effective cyber liability insurance. Pricing of insurance policies depends on many factors, but the use of a SIEM often has a noticeable impact on policy pricing.

Not only is using a SIEM the right thing to do, but the cost of a SIEM may be partially or completely offset by lower insurance costs.

Get started by signing up for our Free Edition, which includes:

- Coverage for up to 3 cloud integrations, including: M365, Duo, SentinelOne, Umbrella, Webroot, Mimecast
- Easy, guided setup in minutes
- Detections automatically rolled out to your account, fine-tuned to filter out the noise
- Summary dashboard of key findings and security reports
- Playbooks with each finding to guide you through response steps
- One week of log data retention -- upgrade for up to one year

Blumira

blumira.com **sales@blumira.com** **877-258-6472**

HOW FIFTHWALL SOLUTIONS CAN HELP

FifthWall Solutions is a cyber insurance wholesaler with near-global access to 40+ carriers. That's about as deep as anyone can get. With our cross-industry insights, we're able to find the best choice for each client regardless of industry, revenue, or past issues with cyber incidents. FifthWall can help your MSP and all of your clients every step of the journey with:

- Evaluations of current policies you or your client may have in place
- Provide side-by-side quote comparisons to find the best options for you
- MSP focused partner program with dedicated insurance partners that can work alongside you and your clients
- Ongoing training, webinars and education to help you stay up to date with all the trends around cyber insurance
- Help drive better cybersecurity tool adoption by finding great rates for your clients when they have the right cybersecurity controls are in place

FIFTHWALL SOLUTIONS

fifthwallsolutions.com

844-719-0981