ARCTIC WOLF

THE LEADER IN SECURITY OPERATIONS

CYBER INSURANCE BUYER'S GUIDE

Evaluate Your Options to See Which Type of Policy Makes Sense for Your Organization

TABLE OF CONTENTS

01 EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

When faced with unrelenting cyberattacks, many organizations turn to their insurance company to cover their losses. In fact, according to the Harvard Business Review, in 2020 the global insurance community saw a cyber insurance program exceed $1 billion for the first time.[1]

While organizations of every size can find themselves under attack, the Hanover Insurance Group found that over 40 percent of U.S. businesses had either no cyber insurance or limits of $1 million or less, which may not adequately cover the cost of the average cyberattack.[2]

In response to the exponentially increasing losses associated with cyber attacks, particularly ransomware attacks where criminals demand a ransom to restore access to networks and data, a growing number of insurance companies faced mounting losses related to their cyber insurance policies and abandoned the sector. In contrast, others reduced coverage, increased premiums, or amended policies to be less attractive.

Why do so many businesses lack coverage, and how can your business secure the cyber insurance it needs?

We created this guide to help you understand the changes to the cyber insurance marketplace and to provide tips on how to qualify and maintain coverage as insurers evolve their approach.

02

WHY INSURANCE COMPANIES ARE REVISITING THEIR APPROACH TO CYBER INSURANCE

WHY INSURANCE COMPANIES ARE REVISITING THEIR APPROACH TO CYBER INSURANCE

Before 2017, most insurers covered ransomware under traditional property and casualty policies.

After the NotPetya attack in 2017, which cost up to $10 billion in global damages, cyber insurers paid out an estimated $2.7 billion to impacted customers[3] and insurers began to change their approach to cyber insurance drastically.

In 2017, run-of-the-mill property and casualty policies began excluding cyber insurance, and dedicated policies covering cyber risk entered the market. Cyber insurance policies written around this time included generous terms and lacked the requirements and oversight embedded in policies today. They were also relatively affordable. This new type of policy allowed risk officers to remove their focus from cyber risk, knowing that policies existed to mitigate their losses. Yet, these policies were part of an unsustainable model, in part due to the increase in ransomware incidents.

Ransomware attacks are unlike other types of insured events that most insurance companies typically cover, such as fire damage in a manufacturing plant. For one thing, there were no observable facts for insurance companies to use to predict ransom amounts. The likelihood of such a cyber incident is also hard to quantify, as it involves deliberate actions by hostile groups whose motivations remain unknown and largely unobservable until an attack materializes. And since most victims negotiated how much they eventually paid in ransom, attackers learned to increase their subsequent demands.

Generous cyber insurance policies also provided attackers with an incentive to attack smaller businesses.

That's because these organizations typically struggle to maintain robust security defenses but possess substantial insurance coverage to cover ransom payments.

Given the growing sophistication, scale, and efficiency of ransomware attacks, coupled with attackers' ballooning extortion demands and pressures from regulators, changes were inevitable. And soon the insurance industry found the need to drastically alter how they structured cyber insurance policies.

+100%

In 2020, standalone cyber insurance direct loss ratios rose above 100% in the U.S. market.

The need for dynamic reappraisal became indisputable in 2020, when several prominent cyber insurers reported that standalone cyber insurance direct loss ratios, which is the share of the company's income paid to claimants, rose above 100% in the U.S. market.

For example, Sompo Group reported a 114% direct loss ratio in 2020, while AIG reported a more modest loss of 101%.[4]

WHY INSURANCE COMPANIES ARE REVISITING THEIR APPROACH TO CYBER INSURANCE

For many insurers, the loss trend continued in 2021.

While most victims pay only a fraction of the ransom after negotiating with cybercriminals, there is nothing to stop attackers from increasing their payment demands. In the first half of 2021, the average ransom demand ranged from $50 million to $70 million.[5]

Some insurance companies have either exited the cyber insurance marketplace or plan to on the near horizon. For example, Axa, one of the largest global insurance groups, announced that it would no longer write new ransomware policies for customers in France.[6]

Others continue to evolve their policies, specifically their coverage and premium rates, as they gain more experience in the marketplace. This includes greater due diligence verifying the security status of the organizations they plan to insure, which can then inform their policy restrictions and premiums.

Additionally, insurers continue to use the reinsurance sector. However, in doing so they must pay as much as 50% of the cyber insurance premium for the right to pass along the risk.

The bottom line?

The spike in the volume of attacks and associated ransom demands required insurance companies to develop a new set of best practices to make their cyber insurance policies profitable, sustainable, and competitive.

03

HOW ARE CYBER INSURANCE PREMIUMS DETERMINED?

HOW ARE CYBER INSURANCE PREMIUMS DETERMINED?

Premiums for cyber insurance continue to increase, from 30% to 45% a year.

Some carriers have started sub-limiting cyber extortion and ransomware, meaning that policyholders can only claim a fixed amount for legal fees, research, forensics, and other remedial costs. Additionally, some insurers apply co-insurance provisions, forcing insured organizations to share more of the risk.[7]

So how do insurers determine the premiums to charge for cyber insurance?

While there's no industry-standard checklist to vet potential policyholders, insurance companies do their best to assess the riskiness of the business, which helps determine the amount of coverage.

Many insurers also administer a cybersecurity questionnaire. The scope and depth of such questionnaires can provide a window into the insurance company's knowledge and understanding of cybersecurity. As is the case with other forms of insurance, more in-depth verification typically occurs when a claims adjuster becomes involved in managing a claim.

Nevertheless, how an insurance company interprets the results of a questionnaire to inform its premium rate calculation remains is unclear, especially if the insurance company lacks the expertise to analyze a company's responses against best practices.

Since the market for cyber insurance is undergoing significant changes, insurance brokers can play an essential role in helping companies secure the best rate. By engaging an insurance broker, companies can request quotes from multiple insurance companies to use as leverage when evaluating policies.

While it may be tempting to select an insurance company that misprices its policy or offers excessive levels of coverage, it's important to remember that it's the claims team, not the underwriting or sales team, that determines whether the insurance company pays a claim.

In addition, low premiums, broad coverage, and security requirements aligned with the business are not the only criteria to consider.

Should a security incident occur, the value of an insurance company extends far beyond the payment of a ransom. It also includes its familiarity with ransomware attacks, ability to coordinate the payment of a ransom expeditiously, and willingness to refer incident response consultants as needed.

04

BEST PRACTICES FOR OBTAINING AND RETAINING CYBER INSURANCE COVERAGE

BEST PRACTICES FOR OBTAINING AND RETAINING CYBER INSURANCE COVERAGE

While the requirements vary by company, cyber insurance underwriters typically expect policy-holders to deploy controls in the following areas:

- Multi-factor authentication
- Secured and tested backups
- Managed vulnerabilities
- Patched systems and applications
- Filtered emails and web content
- Protected privileged accounts
- Protected network
- Secured endpoints
- Logged and monitored network
- No open ports for remote access
- Sunsetting or removal of end-of-life software
- Phishing-aware workforce
- Hardened device configuration
- Prepared incident response

If your company does not have or cannot deliver the controls required by an insurance company, you may struggle to renew an existing policy or be subject to limits on the coverage provided for a ransomware incident. Your company might also experience a significant increase in its premiums or be deemed uninsurable in extreme circumstances.

Therefore, before searching for coverage or readying for renewal, you should assess whether your controls reflect security best practices and suitably mitigate the risk facing your business.

Having foundational elements in place, including relationships with third-party security firms to help deploy and monitor the controls, also makes it easier to respond to requests to incorporate a new control when renewing a policy.

Similarly, you should consider adopting a proactive approach to securing a cyber insurance policy renewal. By contacting the insurance company long before the policy expires, you can discuss the renewal process, including whether you will need to update your control environment to maintain coverage.

If you struggle to achieve budget approvals for security investments, feedback from your insurance company that your organization is unable to obtain sufficient coverage or qualify for a policy can be internal leverage to justify the need to fund security.

05

WHAT IF YOUR INSURANCE COMPANY INCREASES YOUR PREMIUMS OR DROPS COVERAGE?

WHAT IF YOUR INSURANCE COMPANY INCREASES YOUR PREMIUMS OR DROPS COVERAGE?

05

Before accepting a premium increase or losing coverage, ask your insurance company if there's an opportunity to qualify for better rates or retain coverage by documenting your cybersecurity practices in a more rigorous and detailed fashion.

If the insurance company agrees to modify the premiums or leave coverage in place based on additional evidence of a robust security posture, be sure to ask for as much detail as possible about the information you must gather.

Often, this step requires completing a questionnaire provided by the insurance company. Before completing the questionnaire, you should conduct a quick assessment to determine its focus and whether it would paint security in a flattering light.

If the questionnaire portrays your organization's security posture as less than optimal, or the insurance company requires additional security-related investments that are cost-prohibitive or inappropriate for the risks you face, it may make sense to find an alternative cyber insurance provider.

As you comparison shop for a replacement policy, note the type of feedback you receive from insurance companies. If multiple companies ask for a security measure you don't currently have in place, that may be a strong indicator that your approach to security is inconsistent with industry standards.

If you still struggle to achieve affordable premiums or obtain any offer of insurance coverage, you should:

01 Take proactive preventative cybersecurity measures. It's always easier to mitigate risk before a breach occurs.

02 Discuss your options with your cybersecurity partners. They may know about available coverage through preferred insurers.

03 Understand what existing service guarantees (if any) you have that could offset losses in case of ransomware policy limitations.

06

THE ROLE CYBER INSURANCE PLAYS IN ENDING CYBER RISK

THE ROLE CYBER INSURANCE PLAYS IN ENDING CYBER RISK

Arctic Wolf research determined that only 60 percent of organizations have a comprehensive cyber insurance policy to protect them against financial loss from a cyber attack.

Yet, there's some confusion regarding the cost and qualification requirements for cyber insurance.

For organizations without cyber insurance, only 12 percent cite cost as the reason. However, 28 percent believe they do not qualify for any form of cyber insurance. And IT middle management is three times more likely to mention cost for their lack of insurance than C-level executives are, revealing a significant divide between IT teams and executives on the importance of cyber insurance.[9]

While the cyber insurance marketplace is undergoing significant changes, purchasing cyber insurance can help organizations evolve their approach to security, comply with industry best practices, and improve the effectiveness of their security programs.

07 FINAL THOUGHTS

FINAL THOUGHTS

Due to changes in the threat landscape, the cyber insurance industry has responded with drastic changes to how they structure policies to avoid operating at a loss.

Before buying a policy, your organization should understand what its cyber liability insurance does and, more importantly, does not cover. You should also be prepared for a challenging process when buying coverage for the first time and renewing existing policies.

Cyber insurance is not the only protection your organization needs—it's part of a broader security strategy.

When working with insurance companies to initiate or renew coverage, keep in mind that the insurer may have access to qualified security firms to help streamline elements of the underwriting and renewal process. In fact, working with an insurance company's preferred security partner could unlock premium discounts and lessen the time, effort, and expense spent during the renewal process.

A qualified security firm can also provide an insurer with documentation to maintain coverage or avoid higher premiums if your organization must make security-related investments that take time to initiate and deploy. What's more, certain security firms offer supplemental coverage if your company experiences a security incident, assuming you deploy their tools and rely on their services.

SOURCES

[1] https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem

[2] https://investors.hanover.com/news/news-details/2020/Hanover-Study-Finds-Most-Businesses-Insured-Against-Traditional-Cyber-Insurance-Risks---But-Vulnerable-to-Emerging-Risks/default.aspx

[3] https://www.scmagazine.com/news/ransomware/how-the-ransomware-explosion-is-reshaping-the-cyber-insurance-market

[4] https://www.protocol.com/fintech/ransomware-cyber-insurance-premiums

[5] https://securityintelligence.com/news/whats-behind-rising- ransomware-costs/

[6] https://www.protocol.com/why-linkedin-left-china

[7] https://www.insurancebusinessmag.com/us/news/cyber/cyber-insurance-market-reacts-to-ransomware-epidemic-252394.aspx

[8] https://arcticwolf.com/resources/press-releases/arctic-wolf-global-survey-reveals-lack-of-confidence-in-cybersecurity-defenses-and-government-action-amid-fears-of-state-sponsored-attacks

ARCTIC WOLF

SOC2 TYPE II CERTIFIED

AICPA SOC

ISO 27001 CERTIFIED CYBERGUARD COMPLIANCE

CONTACT US

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com

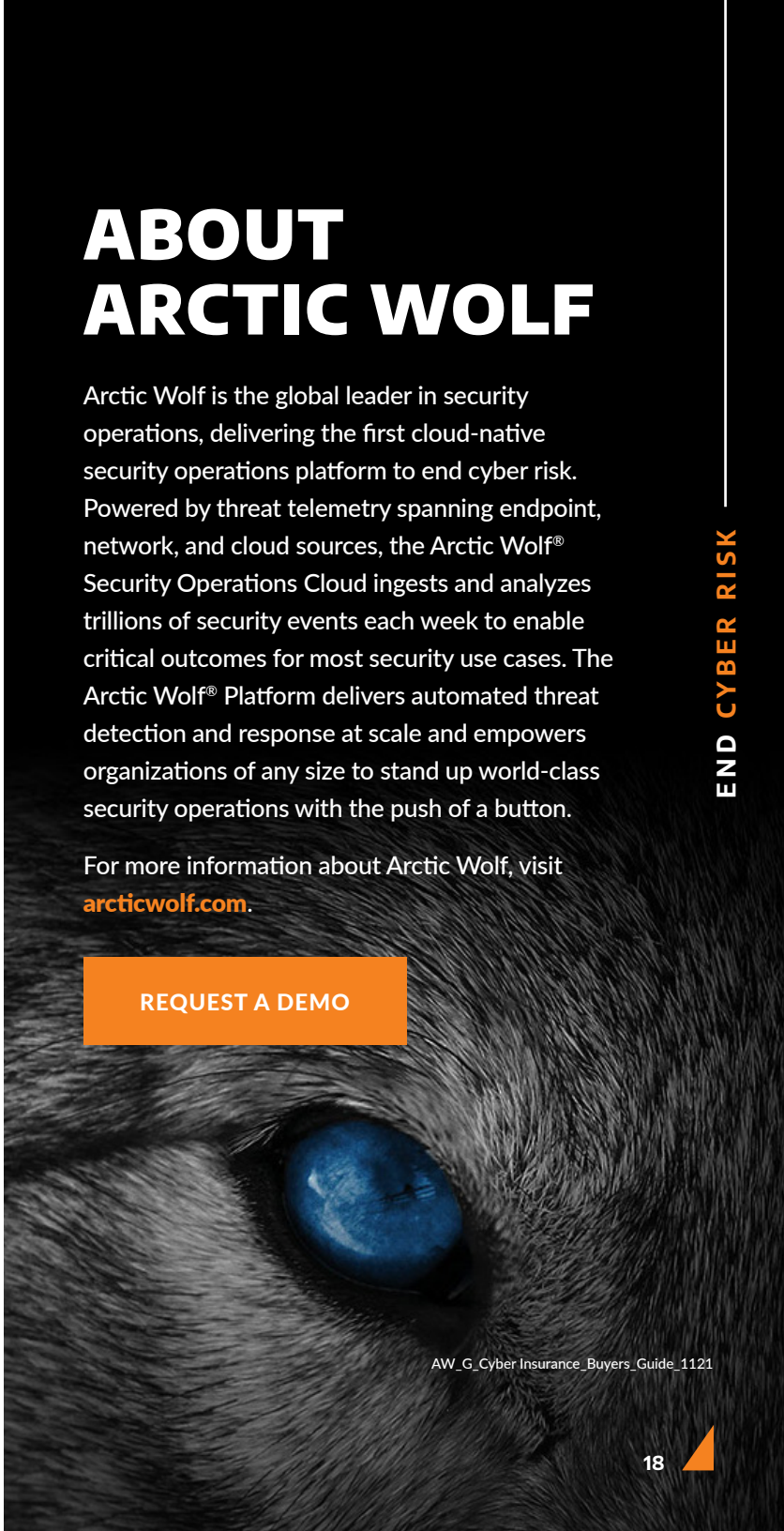
ABOUT ARCTIC WOLF

Arctic Wolf is the global leader in security operations, delivering the first cloud-native security operations platform to end cyber risk. Powered by threat telemetry spanning endpoint, network, and cloud sources, the Arctic Wolf® Security Operations Cloud ingests and analyzes trillions of security events each week to enable critical outcomes for most security use cases. The Arctic Wolf® Platform delivers automated threat detection and response at scale and empowers organizations of any size to stand up world-class security operations with the push of a button.

For more information about Arctic Wolf, visit **arcticwolf.com**.

REQUEST A DEMO

END CYBER RISK



AW_G_Cyber Insurance_Buyers_Guide_1121