ARCTIC WOLF

END CYBER RISK

REPORT

The Global State of Cyber Insurance

Survey shows cybersecurity controls driving the cyber insurance market

Table of Contents

BACKGROUND

When faced with unrelenting cyberattacks, many organizations turn to their insurance company to cover their losses. However, not all organizations are adequately protected.

Recent research 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. In response to the increasingly frequent and more severe cyberattacks, particularly ransomware attacks where criminals demand a ransom to restore access to networks and data, some insurance companies faced mounting losses related to their cyber insurance policies and abandoned the sector. Others reduced coverage, increased premiums, or amended policies to include more stringent risk-mitigation requirements.

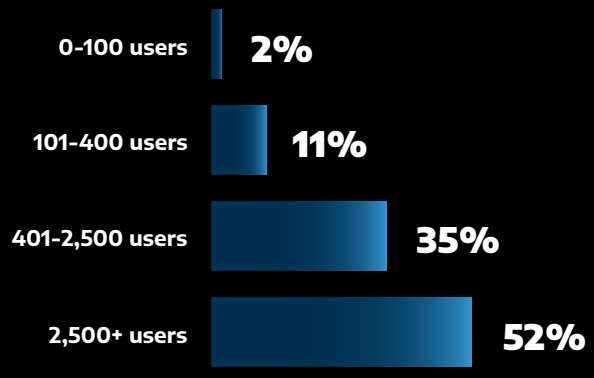
This survey explores how senior IT and corporate executives are grappling with the challenges and changes in the cyber insurance market. We look at how 500 IT and corporate executives from North America, Europe, and South Africa define their cyber insurance strategy, enhance their insurability, and acquire and maintain cyber insurance policies.

Research Methodology

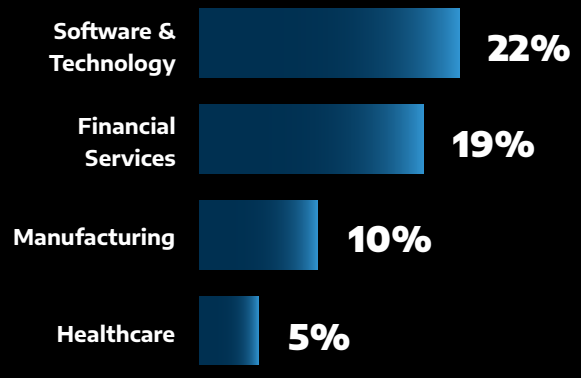
This report is based on the results of a global survey conducted in September 2022 by Energize Marketing among 500 IT and cybersecurity professionals in the U.S. (n=150), Canada (n=50), U.K. (n=100), Germany (n=50), Sweden (n=50), Netherlands (n=50), and South Africa (n=50). Respondents included C-level executives (52%), vice presidents (14%), and directors (34%). The study seeks to identify current cyber insurance trends and cybersecurity controls in place in midsize and larger organizations seeking to renew or obtain cyber insurance.

48% of respondents represented midsize organizations (up to 2,500 employees), and 52% represented large organizations (2,501+ employees). These companies were spread across industrial sectors with software and technology services (22%); financial services (19%); manufacturing (10%); healthcare (5%); retail (5%) the most prominent among them.

Company Size



Industry



EXECUTIVE SUMMARY

Research from Energize Marketing and Arctic Wolf reveals that organizations are becoming more interested in obtaining cyber insurance as a means to transfer risk, especially risk associated with ransomware attacks. Nearly one half of all respondents selected policies that offered 80% to 100% coverage from cyberattacks, with one-third of all respondents reporting that their coverage included full payments of ransoms demanded by the threat actors. The other two-thirds of respondents either had partial-payment policies or policies that did not cover ransom payments.

Concurrent to the outbreak of COVID-19, threat actors began ramping up the number of attacks due to the number of vulnerable remote workforces that needed to be stood up quickly, they increased the amounts of money demanded, and also began deploying the attack strategy known as "double extortion," which further increase pressure of victims to pay a ransom. Although threat actors have not let up on the scope and financial demands, organizations are starting to implement more effective cybersecurity controls. As a result, a relatively small percentage of respondents reported that their efforts to reduce their risk is translating into lower cyber insurance premiums, although the industry is reporting that rates are starting to stabilize and price hikes have decreased.

While rates tended to be significantly higher in 2022, 18% of respondents said they had not experienced any rate increases in the past year and 7% indicated that premiums rose by less than 10%. Globally, the inflation rate for 2022 was 8.8% so a rate increase of 10% or less essentially tracks with inflation. In the United States, the National Association of Insurance Commissioners has reported that cyber insurance loss ratios (a measure of claims loss against premium dollars) has declined in 2021 for the first time since 2017. This is more evidence of a stabilizing market.

In October, *Business Insurance* magazine reported that while cyber insurance buyers likely will see rate increases for their next renewals, "the huge hikes of the past year may be behind them." A side benefit of lower insurance rates is that companies will have more capital to put into investing in cybersecurity controls to reduce their risk, giving them leverage to further lower their rates and secure their environments.

Some 99% of all respondents said they currently have a cyber insurance policy. Of these, two thirds have had their policies for one year or less. While this corresponds to the outbreak of COVID-19 (and its subsequent spate of remote-access based attacks), it also corresponds to the proliferation of Ransomware-as-a-Service, which allowed for ransomware to be deployed more efficiently, and the rise of "big game hunting" ransomware crews like Darkside and REvil, a

practice in which ransomware gangs seek to inflict the maximum amount of harm on an organization and demand a large, multimillion-dollar ransom payment in exchange for providing a decryption key.

Regionally, the statistics are consistent for North America and the United Kingdom. In Germany, none of the respondents have had cyber insurance for more than one year. Interestingly, that differs from Germany's neighbor, Netherlands, where the majority of respondents had their cyber insurance for 1 to 2 years.

In Sweden, the majority of respondents said they had cyber insurance for 1 year or less, while nearly two-thirds of South Africans were insured for 1 year or less with none reporting they had the insurance for more than 2 years.

Key survey findings:

01 The cyber insurance industry is still in a nascent stage. Globally, by an almost 2:1 ratio, respondents said they have had their policies for one year or less compared with those who have had policies for up to two years.

02 Cyber insurance coverage varies by what kinds of losses are covered (e.g., ransomware payments, privacy liability, media liability, network business interruption, etc.) and how much financial coverage each option is offered. 33% of respondents said their policies covered everything, 31% covered everything except ransomware payments, and 30% had additional exclusions.

03 Based on the options respondents selected, 52% expected their coverage to take care of 61%-80% of the costs associated with a data breach. 48% expected the coverage to take care of 81% to 100% of the costs associated with a data breach.

04 Respondents in the United States, Canada, and the United Kingdom invested mainly on multi-factor authentication, email filtering and cloud vulnerability scanning security controls. Respondents in Germany, Netherlands, Sweden, and South Africa included those same security investments, but added cybersecurity controls including managed detection and response, vulnerability scanning, third-party risk management, network hardening techniques, privileged account management, and end-of-life systems management.

05 The cybersecurity controls that were most commonly required by cyber insurance underwriters to maintain a cyber insurance policy included anti-virus software (47%), virtual private networks (41%), cloud monitoring (26%), firewalls (23%), and multi-factor authentication (19%)

06 The highest-ranking motivations to obtain cyber insurance globally were that it is a risk management best practice (38%), it was required by wider insurance policy (34%), and that the board of directors required the organization to secure cyber insurance (26%)

Motivations for Purchasing Cyber Insurance

The top three motivations for obtaining cyber insurance were risk management best practice (38%), a requirement of other insurance, which implies it is a general liability policy (34%), and a board of directors' mandate to become or remain insured (26%). These motivations duplicate the trends of cyber carriers in that rising ransomware incidents and payments drove the desire for cyber insurance. Defending against ransomware is considered a risk management best practice and a business imperative as mandated by the

> **Over the past two to three years, cyber claims have become more frequent than what was seen in the past. Much of this can be attributed to the growth in cyber vulnerabilities for small to mid-sized businesses...It is essential that companies understand the insurance coverage they have purchased and how it can help."**
>
> *Linda Comerford, AVP of Cyber Services and Incident Response at AmTrust,*

What caused your organization to decide to purchase cyber insurance?

Motivations for Purchasing Cyber Insurance

board of directors. In many cases, organizations are contractually required by their business partners to maintain certain levels to spread the risk. While 38% indicated they purchased the insurance because it is a risk management best practice, only 3% specifically called out buying it for its third-party risk management (TPRM) capabilities. This is significant because several insurance industry surveys indicate that some 60% of data beaches are associated with third parties, such as service providers and business partners.

Highly touted security controls that are often considered obligatory by cyber insurers, such as data loss prevention and cyber security awareness training, received much lower citations as key motivators.

Current State of the Cyber Insurance Industry

The cyber insurance market has been in a state of chaos as carriers try to recover from a two-year trend of reducing the size of the policies they write while simultaneously increasing the prices on those policies. At the same time, the number of carriers who are writing cyber insurance policies contracted, although that trend seems to be turning around. The final result: There is a high demand for the reduced supply of available cyber insurance.

While prices are still on the rise, Marsh-McLennan in October announced that policy increases have slowed considerably and a stabilized market is now in sight. Marsh said rate increases for cyber insurance have decelerated nearly 80% on average in just six months. Average rate increases were 54% as of July 2022 compared with 133% at December 2021, according to the *Insurance Journal*.

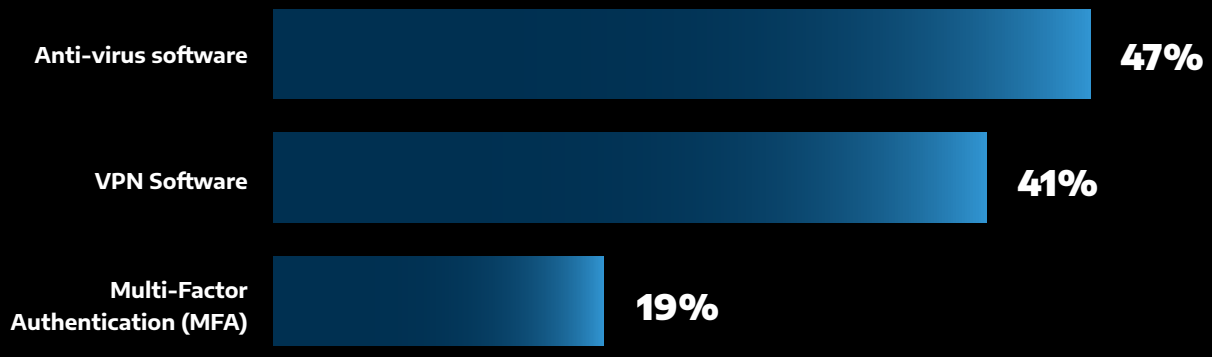
Marsh is not alone in recognizing a restabilization of the market. Insurance broker Risk Strategies also is seeing price increases firming as the market finds its new footing. Like Marsh, Risk Strategies sees companies working harder to develop proactive defenses while enterprises refocus on employing core cybersecurity controls. If this is the beginning of an industry trend — it is still too early to determine if this is a market anomaly or a trend — then the cybersecurity controls market could well be in for significant growth while insurers respond by rewarding organizations with better rates and terms, along with more generous policies.

Cybersecurity Controls to Maintain or Obtain a Policy

Insurance carriers and brokers often require, or at least strongly suggest, security controls that policyholders are expected to have in place in order to maintain their policies. Three of the top five security controls noted by respondents — anti-virus software, virtual private network (VPN) software, and multi-factor authentication — are bare minimums that every company should already have in place regardless of whether they are in the market for cyber insurance. Cloud monitoring and firewalls also are basic controls for protecting the physical infrastructure of a network, be it local or remote.

Organizations interested in addressing underwriters' concerns before they submit an insurance application might consider asking their cyber insurance broker or carrier if they have a list of essential cyber security controls. Implementing these controls before

What systems/processes did your cyber insurance policy require you to maintain to obtain insurance?



Cybersecurity Controls to Maintain or Obtain a Policy

submitting an application potentially could see underwriters acknowledge the proactive security investment by reducing rates or improving terms or coverage limits.

The top five security controls globally that underwriters required in order to maintain or obtain a cybersecurity policy include implementing VPNs (41%), cloud monitoring software (26%), firewalls (23%), and multi-factor authentication (19%).

Globally, these numbers are fairly consistent. Looking deeper into the results, however, there is an interesting anomaly when it comes to firewall security controls. Specifically, Netherlands clocks in at 32% and Canada, Germany, South Africa, and Sweden all are in the 40% range; the U.K. respondents only noted 5% while the U.S. respondents were at 3% for firewalls. The survey did not indicate specifically why the United States and United Kingdom numbers were unusually low for the use of firewalls, but it could simply indicate that firewalls are expected and are not considered unusual enough to call out in these countries.

Cybersecurity Controls to Maintain or Obtain a Policy

In fact, while the U.S. and U.K. tend to emphasize VPNs, anti-virus software and cloud monitoring, Canada and the rest of Europe and South Africa go beyond just those three controls by including firewalls, multi-factor authentication, and vulnerability scanning and management, providing a much broader set of controls to address potential vulnerabilities.

In the National Institute of Standards and Technology (NIST) Cybersecurity Framework, these additional security controls fall more in the category of proactive security, while anti-virus and cloud monitoring come under the category of a reactive response.

"The (NIST) Framework integrates industry standards and best practices to help organizations manage their cybersecurity risks," according to the NIST website. "It provides a common language that allows staff at all levels within an organization—and at all points in a supply chain—to develop a shared understanding of their cybersecurity risks."

The components of the framework are Identify, Protect and Detect, Respond and Recover. NIST further breaks down each of the five categories incorporating the various security controls, helping organizations understand how the various security controls work together in an effective and efficient method. A NIST document that explains the framework can be found here.

Most Impactful Security Controls

When asked which cybersecurity controls had the greatest effect on obtaining or renewing a cyber security insurance policy, respondents cited email filtering (31%), multi-factor authentication (27%), and cloud monitoring (21%).

This was significant because email filtering, an essential security control for weeding out potential ransomware attacks, was tops on the list for helping companies obtain or maintain their policy, but did not rank as high when it came to being *required* to obtain or maintain a policy. Survey results indicate that while not on the required list by insurers to maintain coverage, email filtering is a top security control for reducing risk and thus becoming a better insurance candidate. While this might seem counter-intuitive, it shows that insurers are more interested in results to lower risk than to simply meet required controls.

Although we have seen some recent stabilization in the cyber insurance marketplace, it is not expected that insurance carriers will revert to "pre-2019" underwriting standards where these security control requirements were not demanded uniformly."

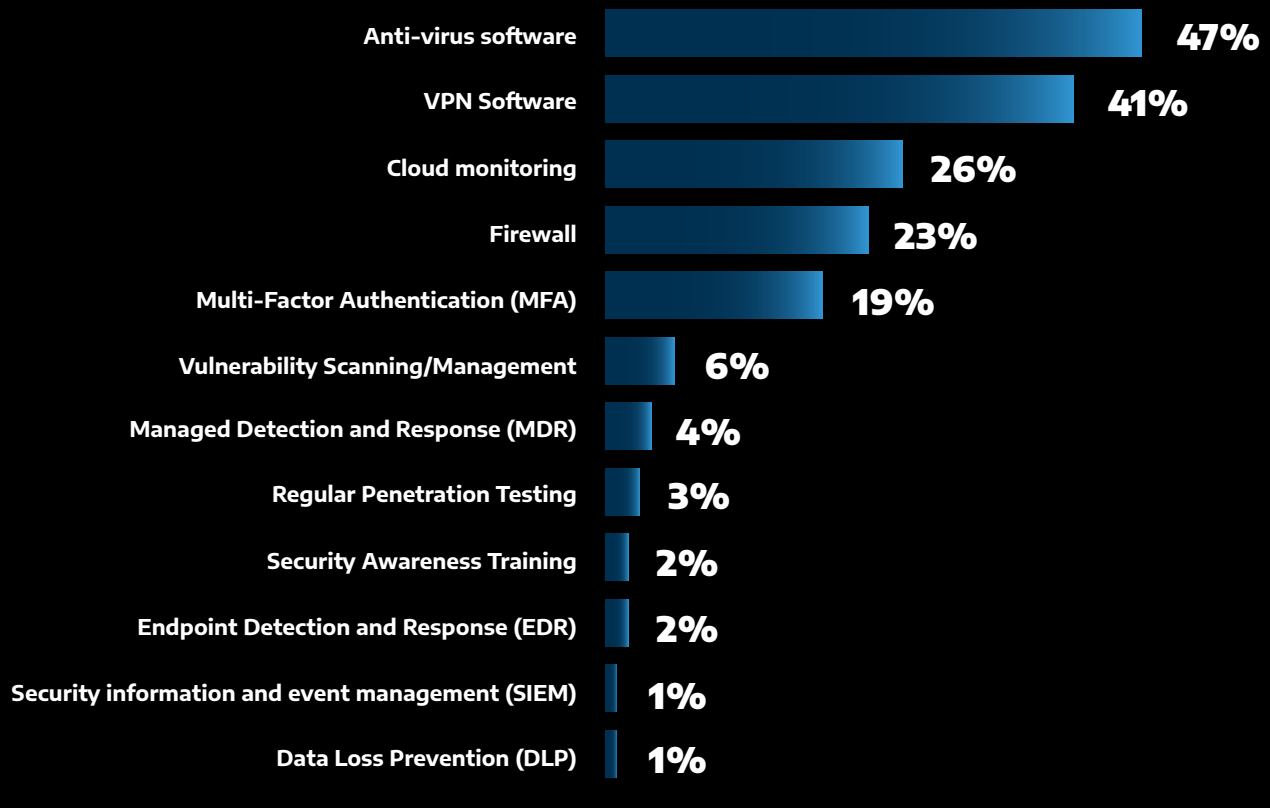
Per Mario Paez, National Cyber Risk Leader at Marsh McLennan Agency

In fact, underwriters tend to evaluate insurance candidates by various criteria. Not only do underwriters look at an enterprise's history of data breaches, they look at how enterprises are becoming better risks in the future by implementing tools and processes to reduce a company's risk profile and potential attack surface, as well as efforts they make to identify and detect breaches before they happen.

Most Impactful Security Controls

Among the security controls that significantly reduce risk are managed detection and response (MDR), on-site and cloud network monitoring, managed risk, and managed security protections. The lower the risk profile of the company seeking insurance, the greater the chance underwriters will approve the application with favorable rates and terms.

What systems/processes did your cyber insurance policy require you to maintain to obtain insurance?



Expectations of Coverage

As with any insurance offering, cyber insurance products range from bare bones to so-called platinum offerings. The lower-end, entry-level packages offerings are endorsements to standard corporate insurance policies, but often exclude, or severely limit, coverage for the more costly cyber incident expenses such as technical incident response costs, legal fees, ransom payments, lost business income, and challenging issues such as ransomware. A more full-fledged solution is a standalone cyber insurance policy with limits devoted exclusively to covering cyber losses, incident response and loss control services tailored for cyber risk, and coverage terms that are drafted with cyber losses in mind.

Survey respondents were nearly split between the levels of insurance they purchase, with just over half, 52%, saying their expectation of coverage is from 61% to 80% of the total cost of a cyber incident. The remaining 48% opted

Given what you know about your cyber insurance policy, what do you expect would be covered in the event of a serious breach?

Expectations of Coverage

for the next higher level that pays up to 100% of a data breach or cyber incident, including coverage for paying the ransom.

While cyber insurance policies vary, there are some common exclusions and one notable new exclusion announced by Lloyd's of London shortly before this survey launched. In August 2022, Lloyd's announced that new policies will have an exclusion for state-sponsored cyberattacks if those attacks significantly impair the ability of a state to function, or significantly impair the security abilities of a state. While it is still too soon to know exactly if and how this exclusion will be exercised, a memo from Lloyd's underwriting director Tony Chaudhry said the company remains "strongly supportive" of the coverage. The change will take effect March 31, 2023, with new policies and renewals of existing policies.

Examples of other exclusions include wrongful acts that occur prior to coverage (for example, a ransomware attack that occurs before the cyber insurance policy is issued), loss of portable devices (some devices might be covered if they are encrypted), security maintenance failures (failures to meet existing minimum standards and compliance requirements), third-party breaches (some third-party risk management is covered but some is not, depending on the carrier), war, invasion, and terrorism. It should be noted, however, that exclusions are a standard part of any insurance policy, cyber or otherwise, so the presence of exclusions should not take anyone by surprise. Exclusions should be read thoroughly by risk managers within organizations to see how they may impact the business' insurance goals.

Coverage Purchased

Survey respondents generally fell into one of three categories in the actual coverage they purchased. One third of the respondents, 33%, opted to cover everything, including the ransom payments. These were among those at the highest level of the 81% to 100% coverage range. Another 31% of respondents opted for coverage for everything except the ransomware payments.

The next level lower, including those in the 61% to 80% range, allowed for other specific costs to be excluded from their coverage. The exact exclusions were not identified in the survey. That said, the more exclusions in the policy the less expensive the policy.

Does your policy cover all cybersecurity incidents you might experience, or does it exclude certain cost categories?

Coverage Purchased

Regionally, 40% of respondents in the United States and Germany fell into the "cover everything" category, with Canada at 34%, South Africa at 30%, United Kingdom at 29%, Netherlands at 28% and Sweden at 24%. Once you eliminate the ransomware payments, from highest to lowest percentage, the ranking is Canada at 42%, Sweden and South Africa at 38%, United Kingdom at 32%, United States at 30%, Netherlands at 26%, and Germany at just 14%.

An interesting observation of Germany responses is that almost half of those respondents, 46%, indicated that their cyber insurance policies had a primary exclusion of business loss; no other region had more than 4% indicating that they had a business loss exclusion.

Does your policy cover all cybersecurity incidents you might experience, or does it exclude certain cost categories?

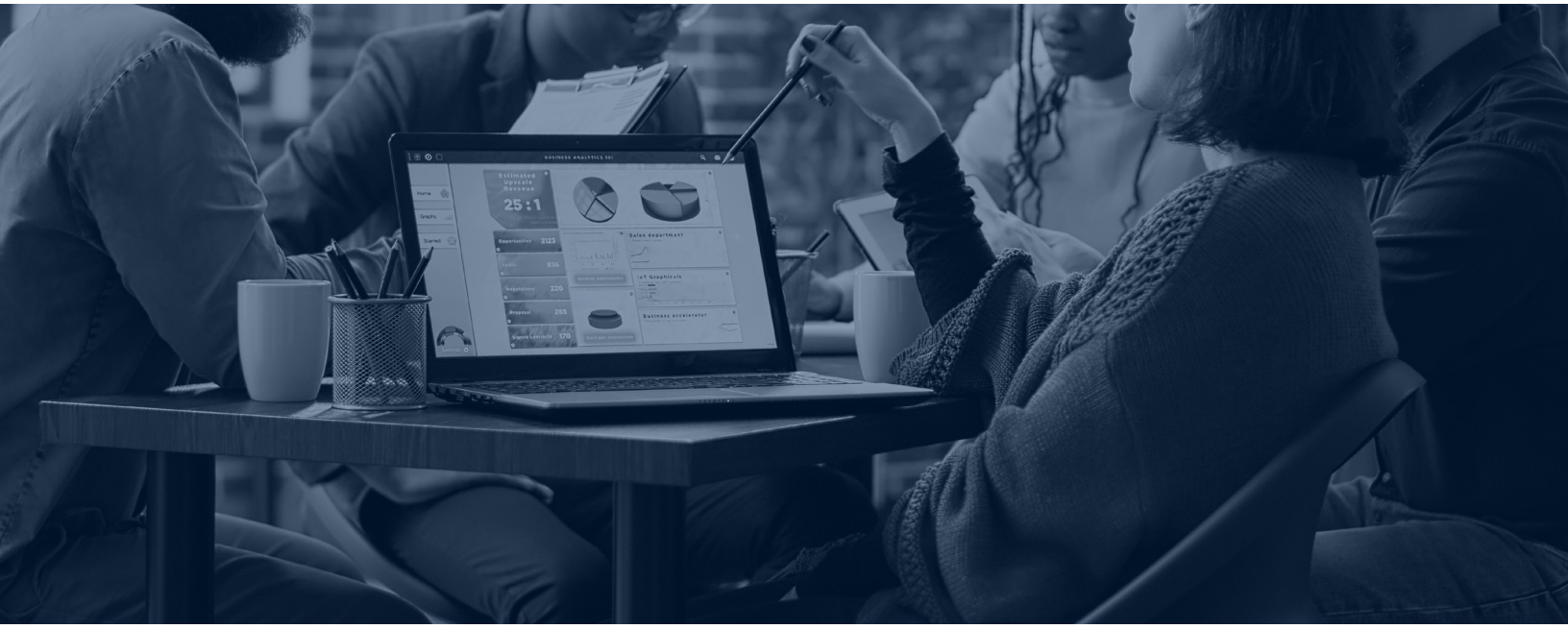
	US	UK	Canada	Germany	South Africa	Netherlands	Sweden
Covers everything	40%	29%	34%	40%	30%	28%	24%
Excludes ransomware payment	30%	32%	42%	14%	38%	26%	38%
Excludes business loss	0%	0%	0%	46%	2%	0%	4%
Excludes other specific costs	29%	38%	24%	0%	30%	46%	0%

Conclusion

Qualifying for cyber insurance today requires a concerted effort by potential policyholders that demonstrates measurable results that produce lower risk.

Respondents confirmed what insurance carriers and brokers have been asserting: Implementing mission-critical cybersecurity controls can lead to lower rates. After all, those who get the best terms, rates and limits will be those who pose the least risk of being breached to the insurance company.

While cyber insurance prices are still going up in many cases, so too are the ransoms being demanded. In order to continue to qualify for the



Conclusion

strongest possible coverage at the most competitive cost, organizations are going to be expected to be able to demonstrate a history of preventing incidents and a plan for strengthening security into the future. A key component of this will be the ability to prevent, identify and mitigate ransomware attacks before they cripple the organization.

An additional consideration is meeting contractual agreements. Many enterprises have contracts with business partners that state the company has cyber insurance to meet certain circumstances. Should a company be unable to obtain or maintain such a policy, they could be in breach of contract with their partners. This furthers the obligation for enterprises to do what they must to obtain the obligatory cyber insurance.

Recent research from Ponemon shows that the average cost of a data breach in the United States is more than $9.44 million, while the global average per breach is $4.35 million.

Recent research from Ponemon shows that the average cost of a data breach in the United States is more than $9.44 million, while the global average per breach is $4.35 million. Once a company has been successfully compromised, additional research shows it has a much greater chance of being breached again. In fact, one

Conclusion

survey showed that 80% of companies that get hit by a ransomware attack get hit again by the same ransomware.

If an organization is underinsured for a ransomware attack, or if it opts for self-insurance and has not set aside the sufficient amount of cash to respond to an attack, it could put a huge strain on the company's finances. In 2018, for example, the City of Atlanta was hit by the SamSam ransomware attack. The attacker's demand was $51,000 in bitcoin. Atlanta chose not to pay the ransom and ultimately paid more than $2.7 million to remediate the attack, although some reports put the overall remediation fee higher.

Some cyber insurance providers are leaving the market, in part because of lower profits from higher ransom payments but others are slowly starting to take their place. Others have been reducing the coverage limits, so some enterprises have been required to obtain multiple policies to cover their risk transference goals. Getting your company's cybersecurity defenses in place and submitting your applications early could help you obtain a policy with the best terms available. If you have questions

> ***If you have questions about what your insurance provider requires, bringing your insurance agent into the conversation sooner rather than later could help you direct your cybersecurity investments to meet the criteria they are setting to qualify.***

Conclusion

about what your insurance provider requires, bringing your insurance agent into the conversation sooner rather than later could help you direct your cybersecurity investments to meet the criteria they are setting to qualify.

While Europeans tend to be more proactive in their defenses than North Americans, it would be folly to assume that either group focuses exclusively on one approach or the other. Everything is a mix; the key is where on the fulcrum sets the tipping point. While not specifically called out in this study, it is important to remember that members of the European Union are subject to the Global Data Protection Regulation (GDPR); in fact, anyone who does business with an EU citizen is subject to that law. That means even though the U.K. is no longer an EU member, GDPR rules still apply. As a result, you will see an emphasis on personal privacy throughout the continent and anywhere a company does business with EU nationals.

There are several ways a prospective insurance client can demonstrate proactive cybersecurity. One method is to partner with a cybersecurity managed services provider that offers 24/7/365 managed detection and response. Another is to employ such proactive security offerings such as Arctic Wolf's Managed Detection and Response, Cloud Detection and Response, Cloud Security Posture Management, Managed Risk, Managed Security Awareness® offerings.

To learn more about how Arctic Wolf can help you reduce your risk and position yourself to better qualify for cyber insurance, call your representative or visit www.arcticwolf.

About Arctic Wolf

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, highly trained Concierge Security® experts work as an extension of your team to help end cyber risk. We make it fast and easy for organizations of any size to stand up world-class security operations that continually guard against attacks in an efficient and sustainable way.

For more information about Arctic Wolf, visit arcticwolf.com