Publication date:
August 2024
Author:
Andrew Braunberg

InsurSec Can Drive An Effective Proactive Security Strategy

How combining proactive security with cyber insurance can help accelerate security maturity

Brought to you by Informa Tech

Commissioned by at bay

Omdia commissioned research, sponsored by At-Bay

Contents

Summary

In the first quarter of 2024, Omdia surveyed more than 400 security decision makers in North America, the UK, France, and Germany. The survey was designed to better understand the current and future use of proactive security solutions, the drivers and inhibitors of market growth and a consolidation of functionality into proactive security platforms, and the role of cyber insurance as a part of proactive security strategy.

The research found that organizations of all sizes see the need for and are embracing proactive security solutions and that cyber insurance is emerging as a key driver of security spend decisions for many organizations.

© 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Embracing proactive security and cyber insurance

Omdia believes the industry is entering a new era that emphasizes proactive security solutions. Preventive and reactive solutions will not disappear, but organizations are shuffling their spending priorities and looking for the better return on investment that proactive security solutions promise to deliver. Omdia's research confirms that organizations of all sizes and geographies are embracing proactive security solutions. More than 70% of respondents have increased spending on proactive security solutions versus a year ago, clearly outpacing spending on preventive and reactive solutions. Proactive security solutions are seen as fostering a comprehensive understanding of the threat landscape and attack surface. As this segment further matures, organizations strongly expect a broader integration of proactive security tools that will further improve attack surface management and security control optimization. A sizable minority of organizations are already deploying proactive security solutions strategically, with larger and more "mature" security organizations leading the way.

The study also found that organizations at every size and level of security maturity experience similar productivity challenges. Dealing with false positive alerts, maintaining legacy infrastructure, and carrying out administrative tasks related to compliance and cyber insurance top the list for organizations of every size. IT/security teams spend less than 50% of their time focused on improving security or helping the business grow, a finding that was remarkably consistent regardless of geography, company size, or a company's security maturity. Companies should take a strategic, proactive approach to security, focusing time and effort on the investments that can most improve the organization's security posture.

Having cyber insurance has emerged as a best practice: 84% of the most security-mature respondents currently have insurance, and 9% are in the process of obtaining it. Overall, 72% of respondents view cyber insurance coverage as critical or important. Though only 13% of all respondents are working "proactively" with their cyber insurance provider to reduce cyber risk, 43% report that cyber insurance requirements are a "major or leading driver" of cyber spend. Thanks to their access to post hoc claims data, hybrid cyber insurance and security firms—"InsurSec" companies—are well positioned to provide timely, relevant insight into the controls proven to mitigate cyber risk and help build a stronger proactive security approach.

Proactive security

Omdia defines proactive security as technologies (including those provided as services) that enable organizations to seek out and mitigate likely threats before they pose a danger to the extended IT environment. Proactive security allows enterprises the opportunity to consistently and programmatically address the specific circumstances—unknown IT assets, vulnerable software, misconfigurations, and the like—that lead to unknown and unexpected threats to the enterprise.

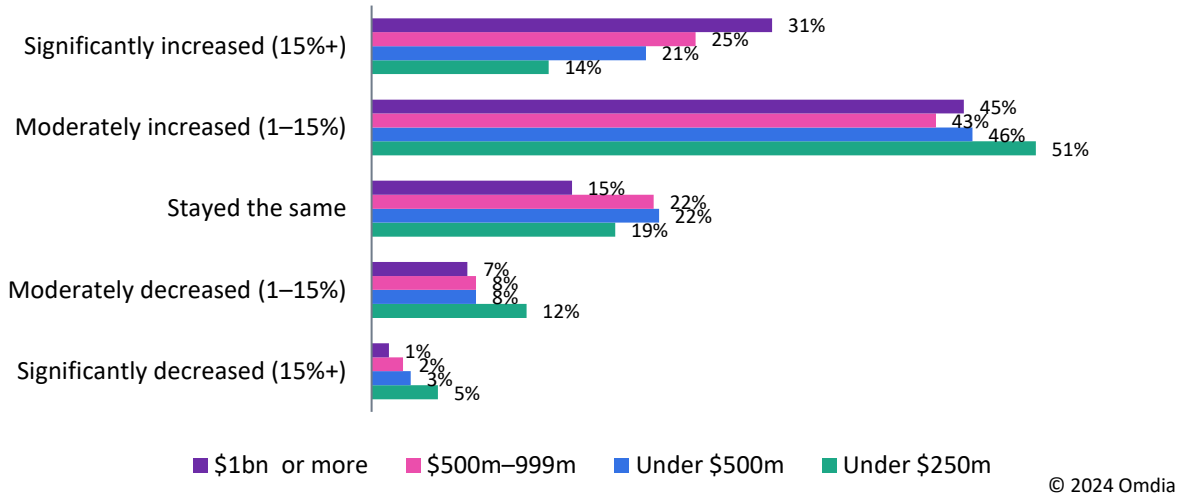
© 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Company size versus proactive security spending

In general, it is true that smaller companies have less budget and perhaps less confidence in where to spend the budget that they have. Both bigger and more mature companies are more likely to have adopted proactive security solutions and to plan on spending more on them in 2024.

Company size is strongly predictive of whether an organization currently treats proactive security investments as strategic components of broader risk reduction programs. As expected, organizations with more mature cybersecurity risk management strategies are also approaching proactive security more strategically. That said, 29% of all respondents are currently approaching proactive security strategically, and an additional 35% describe their approach as semistrategic. This strongly indicates that the use of proactive security solutions is becoming a best practice among the largest and most security-sophisticated organizations.

Figure 1: Year-over-year increase in proactive security budgets by company size



Source: Omdia

Omdia research shows a strong trend toward year-over-year increases in security budgets for proactive security tools. Not surprisingly, larger organizations are more likely to be increasing their proactive spend, but even a majority (65%) of organizations with less than $250m annual revenue report budget increases for proactive security in 2024.

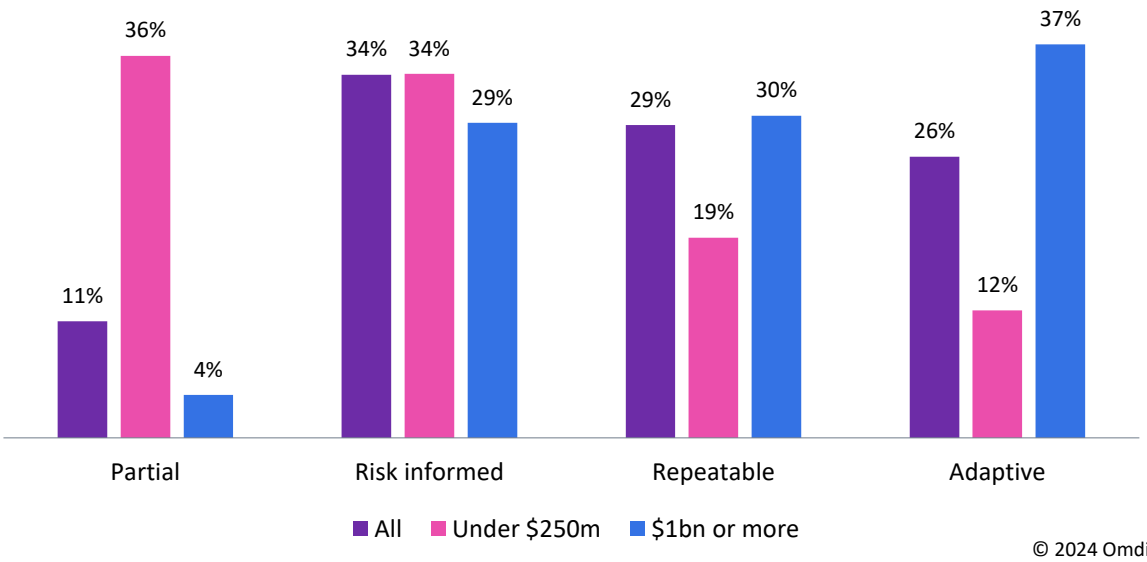
Company size versus security maturity

It is a reality that it takes time and resources to develop security maturity within an organization. This explains, at least partly, why smaller organizations tend to have lower security maturity than

© 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

larger ones. In fact, Omdia's research shows that organizations with less than $250m annual revenue are more than 3× as likely (36% compared with 11%) as all respondents to self-report being at the lowest security maturity level (labeled "Partial" in **Figure 2**). This compares with 17% of organizations in the $250m–500m range and only 4% of organizations with more than $1bn in annual revenue. Conversely, 37% of those largest organizations self-report being at the highest level of security maturity (labeled "Adaptive" in **Figure 2**), while only 12% of organizations with less than $250m in annual revenue report a similar level of maturity. It is important to recognize that though it can be difficult for smaller organizations to achieve relatively high security maturity, it is not impossible. For example, more than 25% of companies with less than $250m annual revenue report taking a "repeatable" or "adaptive" approach to cybersecurity.

Figure 2: Which of the following best describes your organization's approach to cybersecurity risk governance and risk management?



© 2024 Omdia

Source: Omdia

Company size versus productivity challenges

The most security-mature organizations are leading the way in deploying proactive security investments strategically, and the majority (71%) of companies we surveyed had increased their proactive security budget in the past 12 months, but the reality is that even maintaining the security basics remains difficult for businesses of all sizes, not just those with lower security maturity. The leading challenges to productivity for IT/security teams are consistent across all company sizes surveyed. These include dealing with false positive alerts as part of threat detection, investigation, and response activities; maintaining legacy infrastructure, particularly as this relates to keeping up

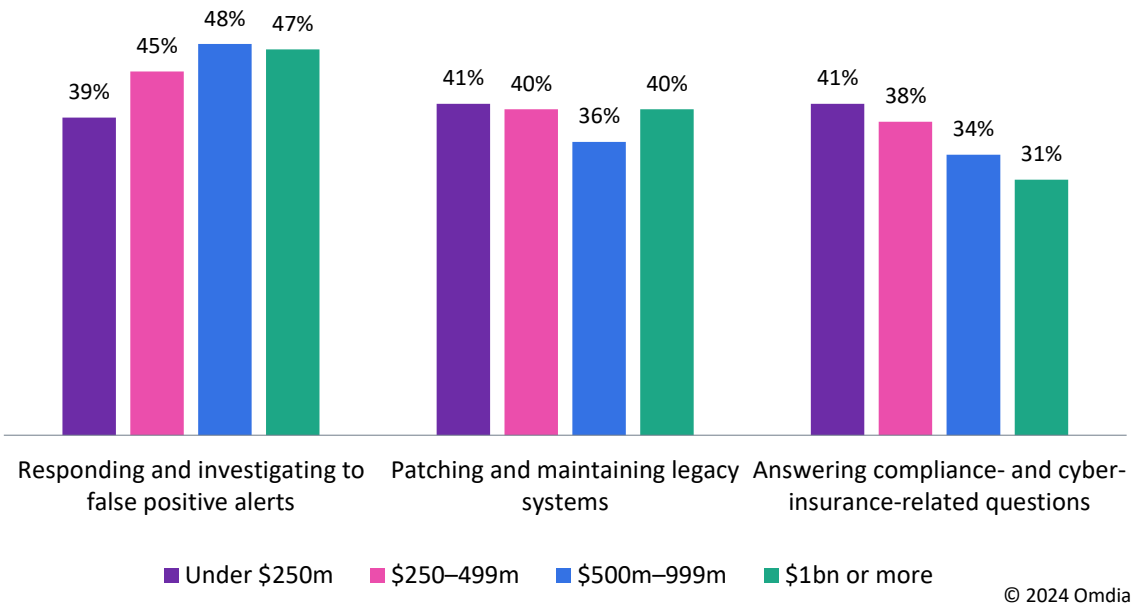
© 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

with vulnerability management programs; and completing administrative tasks related to compliance and cyber insurance (**Figure 3**).

False positives have long been the bane of reactive product suites and contribute to the frustration associated with threat detection and investigation. Similarly, maintaining current infrastructure is a key component of achieving resiliency and consumes much of the time of IT and security teams. (The ability to understand the attack surface associated with this infrastructure and to present a prioritized list of remediation recommendations designed to reduce it is a key capability of proactive security solutions.)

The overhead associated with compliance requirements, of which cyber insurance-related questions can be considered a subset, is also an evergreen challenge. This is not necessarily because of the hours required but rather because of the widespread belief among many security teams that the time could be better spent on activities that improve (not just document) an organization's security posture.

Figure 3: Which of the following challenges are the most detrimental to your IT/security team's productivity?



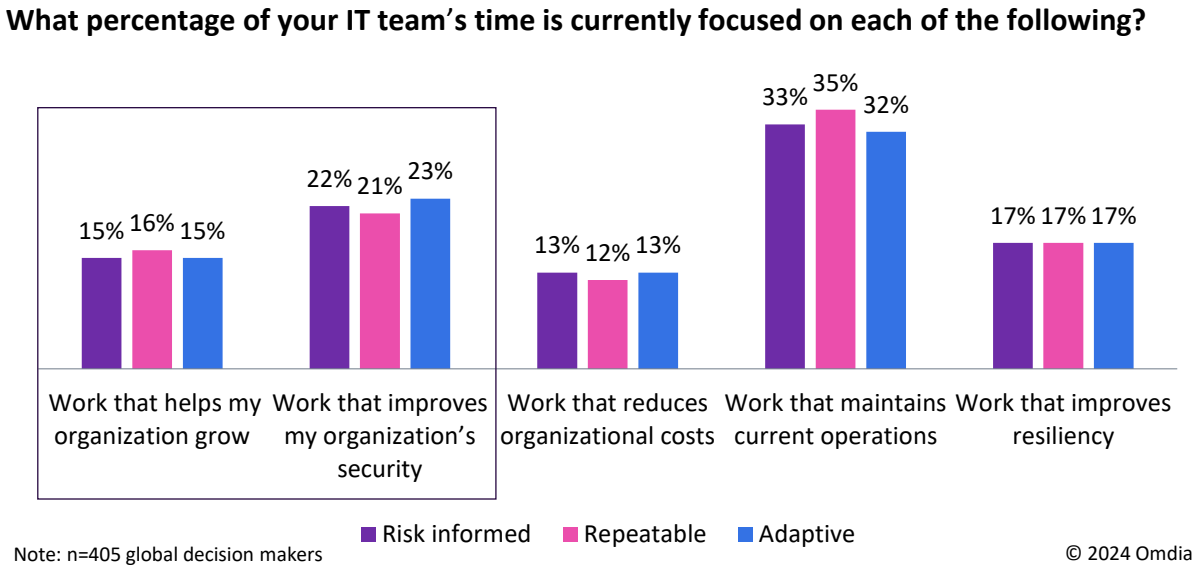
Source: Omdia

In fact, according to our survey, more than 60% of IT/security teams' time is not focused on improving security or helping the business grow, a finding that was remarkably consistent regardless of geography, company size, or a company's security maturity. However, while the kinds of work being done by IT/security teams may be consistent, the outcomes they deliver are not.

© 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Company size is strongly predictive of whether an organization currently treats proactive investments as strategic components of broader risk reduction programs, and as expected, organizations with more mature cybersecurity risk management strategies are also approaching proactive security more strategically (**Figure 4**). The early adoption of proactive security solutions by these more security-mature organizations suggests that a proactive strategy is emerging as a best practice for cyber risk reduction.

Figure 4: Only 37% of IT/security teams' time is focused on improving security or helping their business grow



Note: n=405 global decision makers

© 2024 Omdia

Source: Omdia

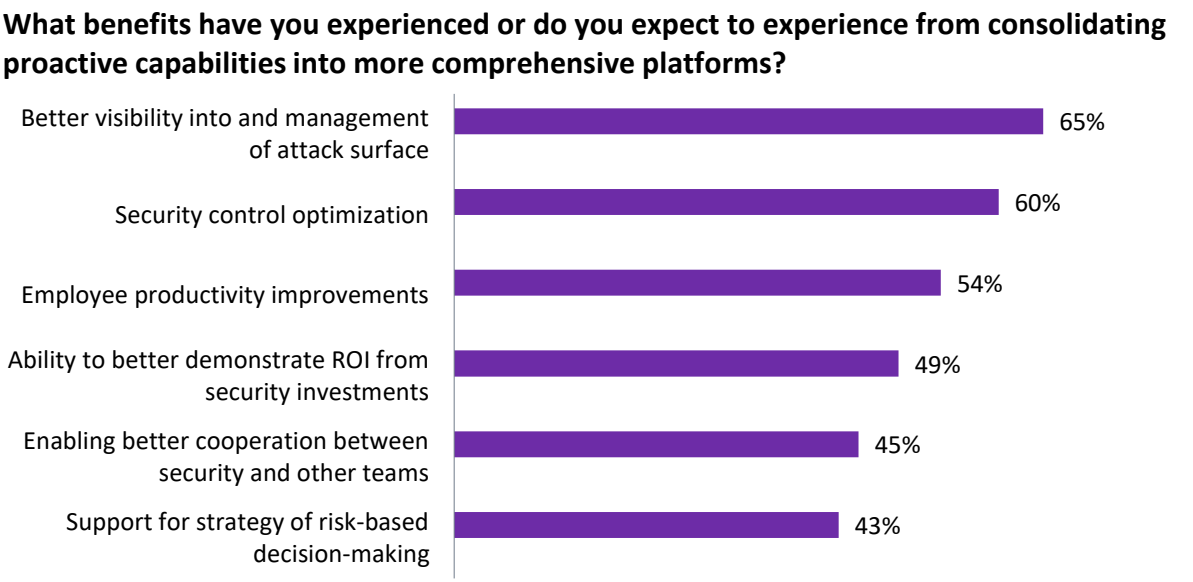
Security practitioners do show interest in ways to work smarter, not harder, when it comes to proactive security:

- Eighty-three percent of respondents are interested in a consolidated platform that combines point solutions such as attack-path management and security control validation with exposure management into a single solution.
- Seventy-one percent of organizations of $1bn or more expect better visibility/management of attack surfaces. Sixty-six percent expect improved security control optimization.
- Employee productivity improvements are expected by 49% of North America organizations and 59% of organizations in Europe, Middle East & Africa (EMEA).

© 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

- Expected benefits hold relatively steady regardless of company size. The top three expected benefits for organizations with less than $250m annual revenue are better management of attack surface (61%), employee productivity improvements (56%), and security control optimization (54%).

Figure 5: Continued consolidation of proactive security functionality is expected to deliver additional benefits



Note: n=405 global decision makers

© 2024 Omdia

Source: Omdia

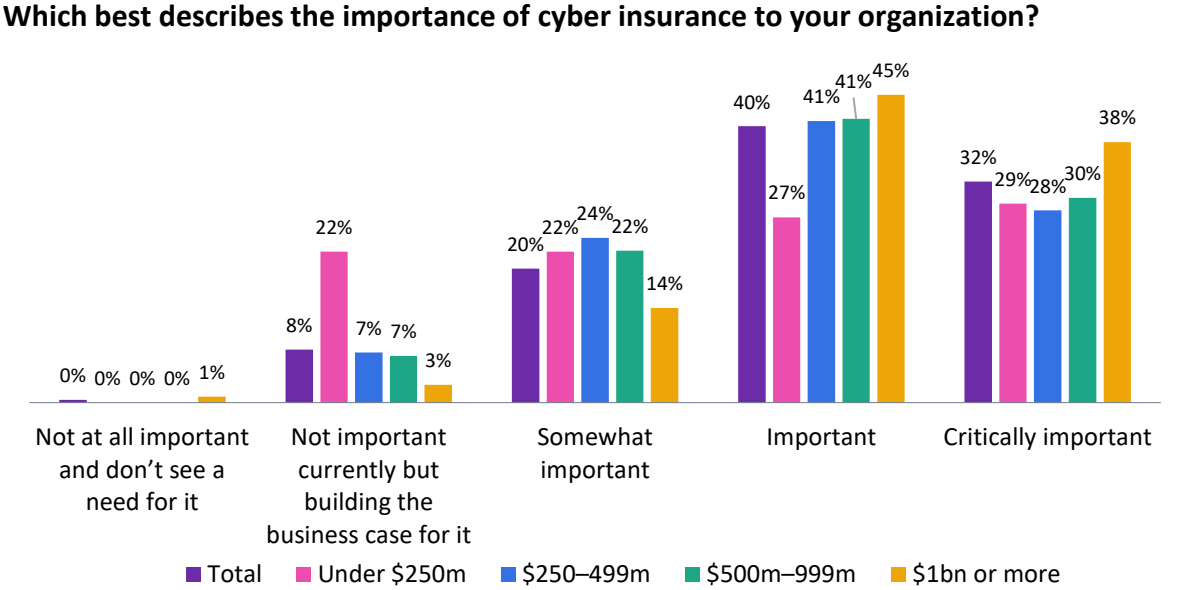
Cyber insurance

With the proliferation of cybercrime against businesses of all sizes in recent years, cyber insurance has become one of the fastest-growing segments of specialty commercial insurance. It has become an increasingly important part of organizations' risk management strategies and has a strong connection to proactive security insofar as both reduce the risk of the organization overall.

For many businesses, cyber insurance has now become a critical purchase, providing a financial backstop in case of a ransomware event or other cyberattack. The most security-mature organizations increasingly view it as a part of the company's overall risk management strategy. In our survey, 72% of all respondents view cyber insurance as critical or important to their organization, and fewer than 10% view it as unimportant.

© 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Figure 6: Seventy-two percent report that cyber insurance is important or critical to their organization



Note: n=405 global decision makers

© 2024 Omdia

Source: Omdia

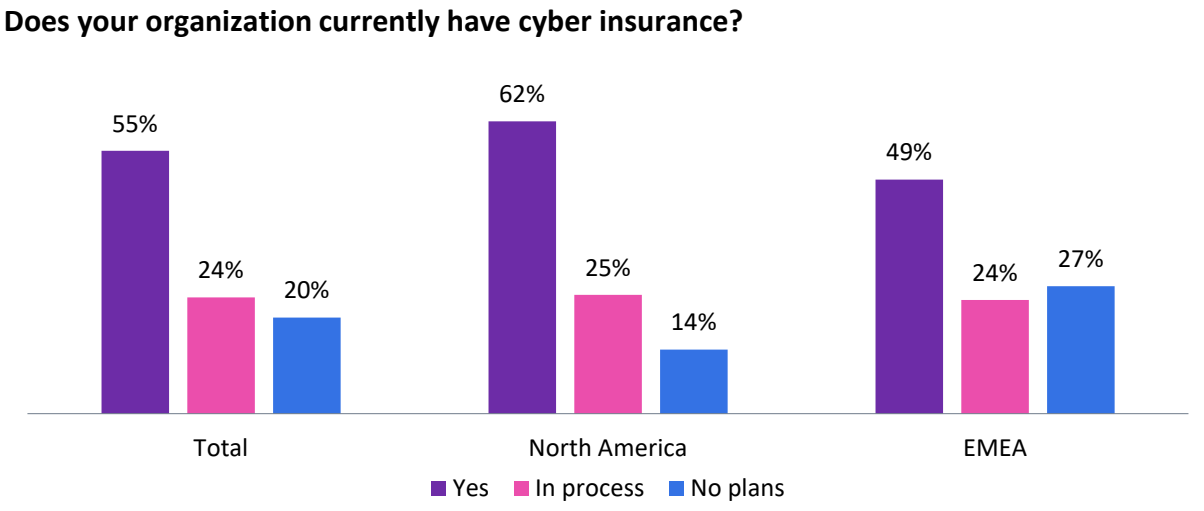
Not only do most companies see cyber insurance as important, cyber insurance requirements are a major factor in how organizations make security-buying decisions. Forty-three percent of all respondents report that cyber insurance requirements are a "major or leading driver" of cyber spend. (Let that sink in for a minute.) The percentage is even higher among the largest organizations, among which 52% report that cyber insurance requirements are a major driver of spending. Only 22% of organizations with less than $250m in annual revenue report the same.

Cyber insurance adoption

Seventy-nine percent of respondents currently have cyber insurance or have plans to acquire it in the next 12 months. The North American market appears to be ahead of the European market in cyber insurance adoption, with North American organizations 25% more likely to report having cyber insurance than their European counterparts (**Figure 7**).

© 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Figure 7: Only 55% of organizations currently have cyber insurance



Notes: n= 405 global decision makers. North America: US and Canada; EMEA: UK, France, and Germany

© 2024 Omdia

Source: Omdia

Smaller and less mature organizations are much less likely to have cyber insurance. For example, only 37% of organizations with less than $250m annual revenue currently have cyber insurance. These organizations also seem the least likely to understand its value. Omdia research shows that 22% of organizations with less than $250m annual revenue do not currently see cyber insurance as important, and another 22% view it as only somewhat important. On the other hand, organizations that self-report a high level of security maturity are much more likely to have cyber insurance (84%).

Not every organization can find an insurer, of course, but this data suggests that not all organizations yet view cyber insurance as a key component of broader cyber risk management strategies. When they were asked what role cyber insurance plays in organizational management of security risk, just over half (52%) of respondents reported that cyber insurance is simply a compliance requirement or a reactive financial backstop.

However, cyber insurance can be an important driver of security and decision-making controls, both as “carrot” and as “stick.” Forward-thinking cyber insurers—frequently referred to as InsurSec companies—are actively leveraging their comprehensive data about their insureds’ cyber risk. InsurSec firms both require security controls that their data has shown can reduce risk (the stick) and want to proactively identify areas where companies can get ahead of their risk and advise clients on their security posture (the carrot). This consultative approach has strong alignment with proactive security insofar as both reduce the risk to the organization overall.

This InsurSec approach remains out of reach for many IT/security teams. Only 13% of all respondents work “proactively” with their insurer to reduce cyber risk. A healthier 33% identify preventive measures for cyber risk “with support from” their cyber insurer. The rate of proactive collaboration

© 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

is even lower in many critical-infrastructure sectors, where cyber risk has potential for even larger societal impact. For example, it includes only 4% of manufacturing companies; 7% of energy, utility, and transportation companies; and 8% of healthcare companies. This seems a missed opportunity on both sides of the insurer/insured relationship.

Omdia believes this is an important finding and that there are many organizations that would benefit from partnering with a cyber insurance provider to help drive security maturity.

Less security-sophisticated organizations, in particular, need advice regarding how to cost-effectively work toward a better, more proactive security posture, while enterprises can benefit significantly from aligning proactive security spending with cyber insurance requirements.

An emerging option is to partner with an InsurSec company. These relatively new entities combine cybersecurity products and services with insurance offerings to offer comprehensive prevention and protection.

Aspirational security

The days when organizations could assume that only Fortune 100 companies are targeted by malicious hackers are long gone. Today, many of the core cybersecurity challenges confronting organizations are similar, regardless of their size. The scale of the problems might differ, and of course organizations of different sizes have varying budgets, resources, and internal expertise, but IT and security teams are remarkably consistent in terms of how they spend their time, regardless of any demographic or “firmographic” profile.

Omdia strongly asserts that even smaller and less mature organizations can achieve better security posture with proactive security solutions. Best practices regarding the use of proactive security solutions are still being determined, however, and the amount of guidance related to the use of proactive security tools is limited, particularly in comparison with the use of preventive and reactive tools.

Smaller and less mature organizations, which typically have less internal security expertise, are liable to fall further behind in the adoption of proactive tools and the development of proactive strategies. These organizations clearly need help in determining how to invest in proactive security solutions strategically. Cyber insurers, especially those that take an InsurSec approach, should be an obvious resource for advice on where and when to invest in proactive security solutions. This, unfortunately, is not universally the case.

For most organizations, cyber insurance should be seen as a key component of cyber risk management strategies. InsurSec providers are increasingly well positioned to act as data-driven experts in assessing cyber risk. Risk will always remain a key determinant for an insurer, but many organizations would do well to view their insurers as potential strategic advisers with respect to security investments and broader cyber risk strategies.

© 2024 Omdia. All rights reserved. Unauthorized reproduction prohibited.

Appendix

Definitions

Cybersecurity products and services can be broadly classified depending on how they approach the problem of keeping data and infrastructure safe from attackers. Omdia splits the entire universe of security solutions into three categories:

- Preventive products and services add layers of security (traditionally referred to as defense in depth) that compensate for weaknesses and exposures in the people, processes, and technology that digital infrastructure comprises.
- Reactive solutions search for indicators of compromise that are used to determine where preventive solutions failed or were bypassed and to quickly determine how to shut down and remediate attacks.
- Proactive security solutions, however, search for indicators of exposure and recommend and perform actions to eliminate or mitigate those exposures before they are exploited. Omdia includes the following solutions within the proactive category: attack surface management, risk-based vulnerability management, security posture management, incident simulation and testing, penetration testing, and red teaming among others.

One of the benefits of categorizing the solution market based on these three categories is that it broadly aligns with the evolution of cybersecurity. When the digital age dawned, it was thought that preventive products would ward off all bad actors. While preventive solutions continue to be deployed broadly and serve an important purpose, alone they are not sufficient. Then came the era of assuming breaches and building security operations centers as the focus shifted to the deployment of reactive solutions. Though threat detection, investigation, and response (TDIR) solutions are still needed, the limits of these reactive approaches to security are clear: finding and remediating critical threats at scale is costly, complex, and prone to frequent failure. Omdia believes the industry is now entering a new era that emphasizes proactive security solutions. Preventive and reactive solutions will not disappear, but organizations are shuffling their spending priorities and looking for the better return on investment that proactive security solutions promise to deliver.

Cyber insurance

Cyber insurance is a specialized insurance product designed to provide financial protection to businesses in the event of cyberattacks, data breaches, or other cyber related incidents. This type of insurance offers coverage against a wide range of cyber related risks, though the specifics vary by policy. Businesses of all sizes that rely on digital systems, store sensitive information, or even simply have an online presence can benefit from the protection provided by a cyber insurance policy. At its core, cyber insurance helps businesses react in a timely manner and then recover from a covered incident. Policies typically provide financial support for investigations, data recovery, legal defense, and even public relations efforts to restore a tarnished reputation.

Methodology

While the cybersecurity industry has clung to the "assume breach" mantra with its preventative and reactive solutions, organizations are awakening to a smarter strategy: proactively understanding attack surfaces, mapping attack paths, and plugging vulnerabilities to prevent breaches. While a host of standalone proactive tools have been available for many years, proactive security platforms are emerging that can provide much more holistic risk discovery, prioritization, and automated remediation.

In 1Q24, Omdia fielded a custom survey to 405 global security decision makers to better understand the current market landscape and approaches, investment trends and preferences, attitudes towards risk management and organizational pain points associated with proactive security. Respondents included decision makers from North America and EMEA, at SMB+ sized companies across a variety of industries. Respondents included individuals from manager level through C-level positions, who have responsibility for cybersecurity product investment decisions.

About At-Bay

At-Bay is the InsurSec provider for the digital age. By combining world-class technology with industry-leading insurance and security expertise, At-Bay was designed from the ground up to empower businesses of every size to meet cyber risk head on. Our InsurSec approach provides end-to-end protection for modern businesses. It's a force multiplier that includes security, threat intelligence, and human experts to close the SMB cybersecurity gap—all as part of their insurance policy.

Author

Andrew Braunberg
Principal Analyst, Cybersecurity
customersuccess@omdia.com

Get in touch

www.omdia.com
customersuccess@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa Tech and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.