INFORMATION SECURITY AND CYBER RISK MANAGEMENT

The tenth annual survey on the current state of and trends in information security and cyber risk management

OCTOBER
2020

Sponsored by

ZURICH

In the tenth year of the annual Information Security and Cyber Risk Management Survey from Advisen Ltd. and Zurich North America, we see the cyber insurance market fully coming into its own as a necessary component of any commercial insurance program. This year's survey shows buyers who feel more confident than ever about their coverage needs, the perceived cost of their risk, and their preparedness for cyber events.

More respondents than ever — nearly 80 percent — carry cyber insurance, with 55 percent buying stand-alone policies. This take-up rate for cyber insurance has steadily climbed since 2011, the first year of our survey, when just 34 percent of respondents bought some type of cyber coverage. Cyber insurance is no longer a luxury item, even amid a hardening overall insurance market. As the percentage more than doubled over the last decade, the results illustrate just how essential insurance buyers consider protection against cyber events to be. For the outliers (approximately 12 percent of respondents do not have cyber insurance or are in the process of buying it), many say price and buy-in from the C-suite and IT professionals in their organizations are their biggest obstacles.

Proving the value of cyber insurance, more respondents than ever reported they had filed a claim (over 50 percent) and for 74 percent of those respondents, the claim was covered by their insurance.

We see signs of, if not hardening, at least some tightening of the cyber insurance market in terms of price and heightened underwriting discipline. We also see areas where even sophisticated buyers might need some guidance on their approach to cyber security, communication with other stakeholders, and breach preparedness.

SURVEY HIGHLIGHTS

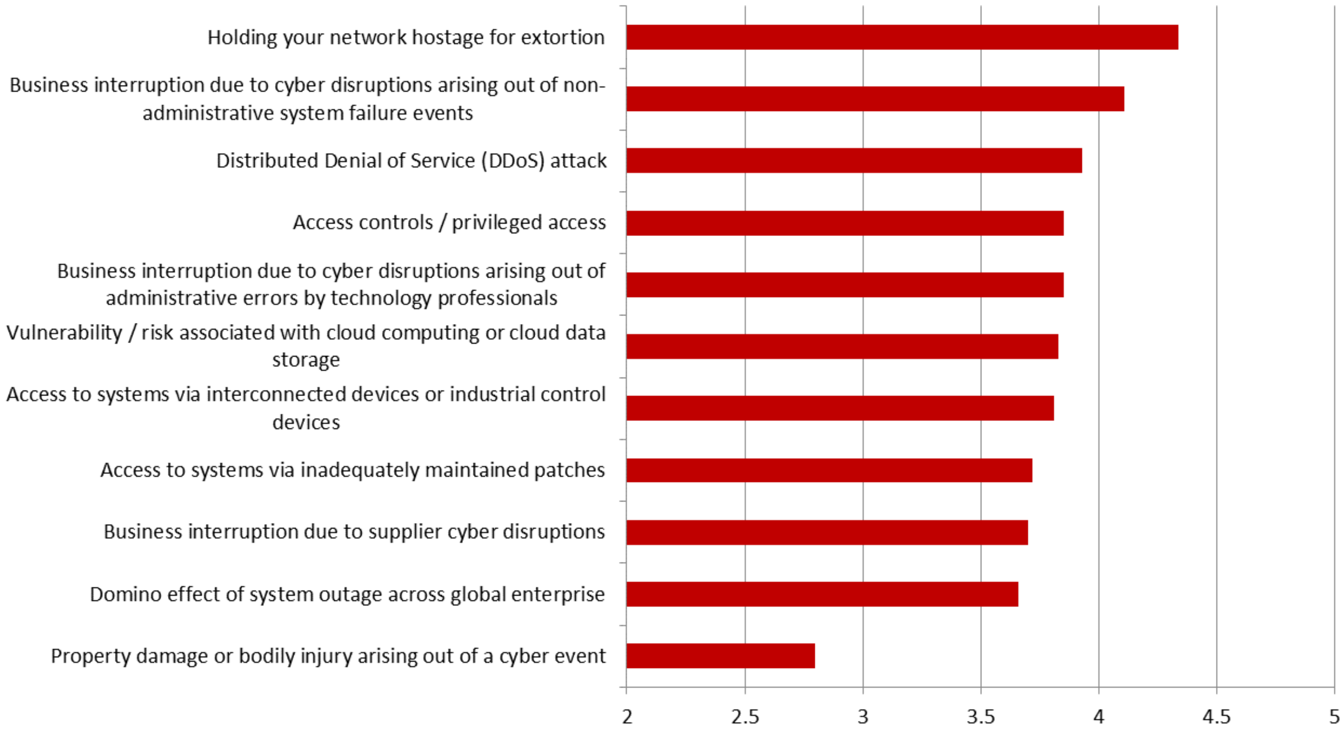
- This year’s survey features the highest percentage of cyber insurance buyers ever – nearly 80 percent carry some level of cyber insurance (55 percent of respondents with cyber coverage have a stand-alone policy).
- Buyers have high expectations for their cyber insurance – Data breach is the number-one most expected coverage for 97 percent of respondents, but cyber extortion/ransomware is close behind at 94 percent, followed by data restoration at 91 percent.
- Business interruption is viewed as the worst outcome of a ransomware event by 43 percent of respondents; reputational harm was cited as the second-worst outcome by 29 percent, and other outcomes such as loss of data (15 percent) and loss of funds/paying the ransomware (11 percent) were viewed as far less impactful.
- Sixty percent of respondents feel either “extremely prepared” or “prepared” to respond to a ransomware event, while 33 percent feel “somewhat prepared.”
- Well over half of the respondents who filed a cyber claim (64 percent) were either “very satisfied” or “satisfied” with the outcome of the claims process. Another nine percent were “somewhat satisfied” and 12 percent were some level of dissatisfied.
- Just over a third (35 percent) of respondents provide annual training for employees on cyber risks, while 24 percent conduct quarterly trainings.
- Similarly, 30 percent of respondents only assess their company’s exposure to cyber risks on an annual basis, indicating potential gaps in security.
- 81 percent of respondents have not changed their cyber security spend, despite financial constraints due to COVID-19. Last year’s survey revealed boosting cyber security budgets as a priority and the lack of change amid the pandemic marks a positive sign.

DISCUSSION OF FINDINGS IN DEPTH

Perceptions of Risk

With a more sophisticated survey sample (as evidenced by nearly 80 percent of respondents carrying cyber insurance), it stands to reason respondents are more able to identify the cyber risks facing their organizations. For example, cyber-related business interruption ranks as a top concern in this year's survey as in last year's, but "Having your network held hostage for extortion" ranks higher than either business interruption or contingent business interruption. Distributed Denial of Service (DDoS) attacks (a malicious event that disrupts normal web traffic to a site) rose significantly in the year-over-year ranking, now third to cyber extortion and business interruption.

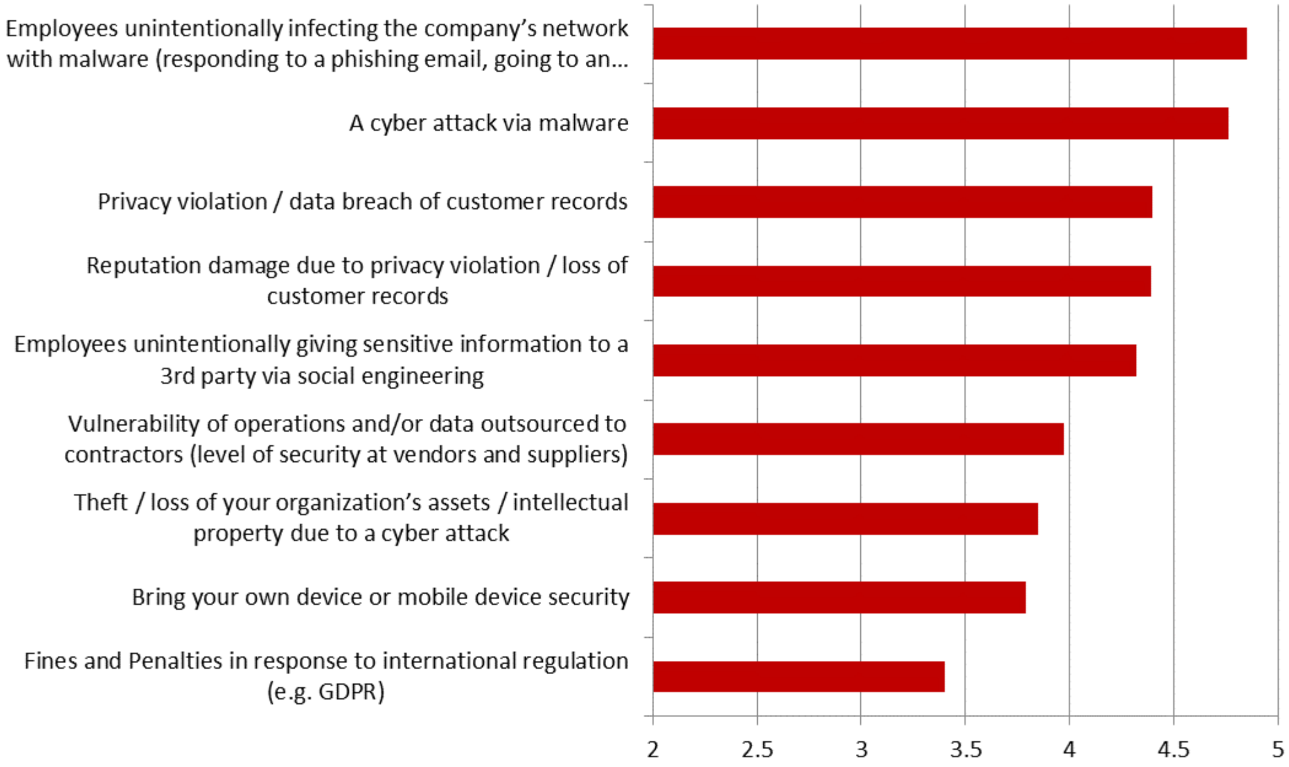
FROM THE PERSPECTIVE OF YOUR ORGANIZATION, ON A SCALE FROM ONE (LOW RISK) TO SIX (HIGH RISK), PLEASE RATE EACH OF THESE BUSINESS CONTINUITY RISKS



These results offer excellent insight into how well respondents understand the cause-and-effect relationships of cyber events and how much public attention to cyber risks has increased. As could be expected by the tremendous rise in ransomware events over the last year and increased media attention to cyber attacks against cities, schools and hospitals, fear of having to decide whether to pay a ransom to rescue encrypted data weighs heavily on organizations. The financial impact, media fallout, and potential legal issues of such events also likely elevate cyber extortion events above cyber incidents that only cause business interruption. The results show the increasing nuances of how organizations think about cyber risk – they understand not only what their biggest consequences might be, but which types of cyber events can bring about those outcomes. Since DDoS attacks and cyber extortion can both disrupt the normal flow of business operations, those possibilities are top of mind for risk managers.

Similarly, respondents see a clear link between their employees and potential cyber events, especially amid the COVID-19 pandemic and remote work structures. Respondents ranked “Bring your own device” as their second-lowest concern in terms of data integrity risks, but they ranked “Employees unintentionally infecting the company’s network with malware” and “Employees unintentionally giving sensitive information to a third party via social engineering” much higher, suggesting organizations understand user error is far more likely to cause a security problem than the devices workers use.

FROM THE PERSPECTIVE OF YOUR ORGANIZATION, ON A SCALE FROM ONE (LOW RISK) TO SIX (HIGH RISK), PLEASE RATE EACH OF THESE DATA INTEGRITY RISKS



While understanding the risk presented by human error, even sophisticated cyber insurance buyers may not realize the level to which employees can be as much the solution as they are the problem. The survey results show respondents could be paying much more attention to assessing their risks as well as providing more regular training for workers.

“Annually” was the most common answer for respondents on how frequently they train their employees on cyber security at 35 percent, followed by “Quarterly” for 24 percent. Those respondents conducting quarterly cyber security trainings, along with the nine percent who conduct monthly workshops, are on the right track. For those doing only annual reminders — and the 13 percent who conduct training less than once a year — there’s room for improvement, especially with such concern over the “human element” of risk.

Knowing which topics to train employees on is just as important as knowing when to offer training and this year's survey offered interesting insight into how frequently respondents assess their exposure to cyber risk. Less than a third of respondents (30 percent) assess cyber risks to their organizations monthly. Another 30 percent only perform assessments on an annual basis. Despite recognizing the consequences stemming from cyber events, organizations may not realize how rapidly cyber risks can evolve. Just in the last year, for example, ransomware actors have shifted to exfiltrating data from their targets, turning such events into not only extortion/business interruption scenarios, but also potentially notifiable data breaches. Assessing risk exposure should be performed annually at a minimum, but organizations should more regularly monitor for new threats in this changing environment.

One notable result indicates respondents ranked vendor risk assessment second lowest among their cyber risk management strategies, preferring instead to focus on internal assessments. Reliance on third parties frequently provides efficiency in business operations but can also create additional cyber risk. Given the concern over business interruption and contingent business interruption, assessing supply chain risk should be a key part of strategy. On the positive side, the vast majority of respondents (84 percent) say cyber risk has become a much more significant concern and they've taken the necessary steps to address it (including investing in cyber security solutions (56 percent), partnering with outside firms to improve cyber defenses (52 percent), and having risk management and IT work together on the risk (51 percent).

One notable result indicates respondents ranked vendor risk assessment second lowest among their cyber risk management strategies, preferring instead to focus on internal assessments.

Engaging the Stakeholders

Ensuring information security and cyber risk management requires buy-in from all stakeholders across an organization. This year's survey revealed, as earlier surveys have, respondents feel risk management (81 percent) and IT professionals (85 percent) view cyber threats as a significant risk.

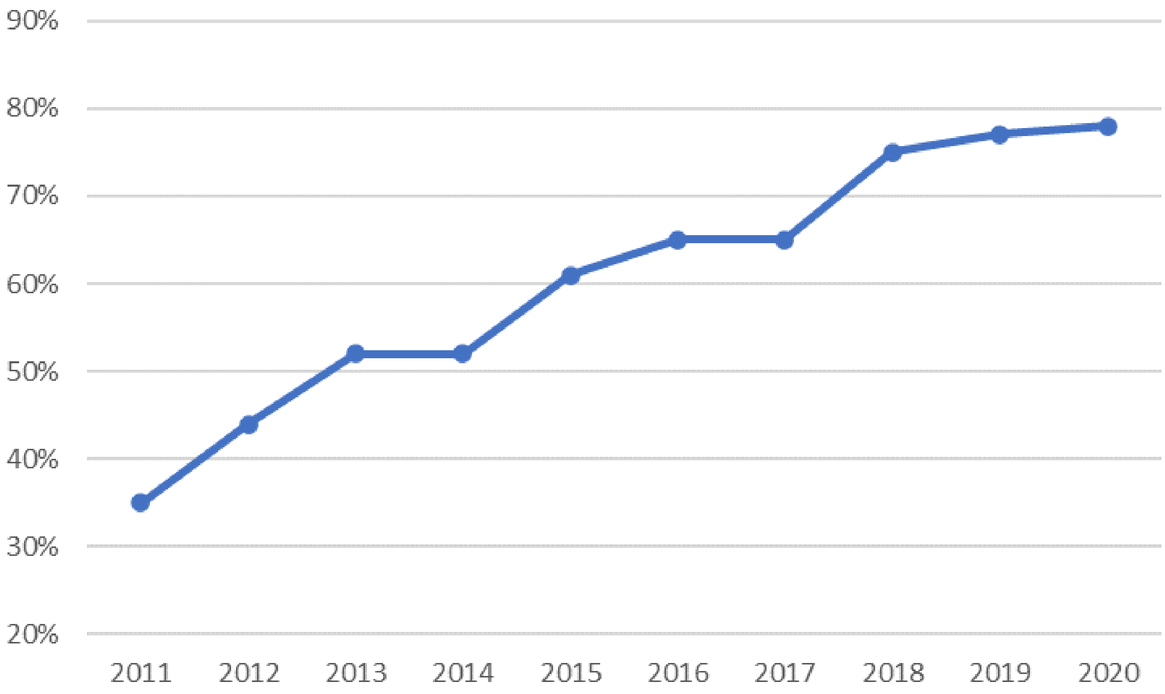
According to the survey, boards and C-suite execs view cyber risks as a significant threat to organizations (71 percent and 70 percent) more than ever, but still at lower levels than IT professionals and risk managers/insurance buyers. However, risk managers may find boards and executives are much more concerned about cyber risks than risk managers perceive. Large-scale cyberattacks and critical infrastructure breakdown have ranked as a top 10 risk for executives for several years, according to the World Economic Forum's annual Global Risks Report.

More communication and discussions on cyber risk between risk managers, insurance buyers, and executives can create a more meaningful, enterprise-wide strategy. The concern is there on the part of the C-suite and boards, but risk managers may need to draw a clearer line between the cyber risks facing the organizations and the solutions available through insurance and pre-breach preparation.

A Growing Insurance Market

With heightened awareness of cyber risks comes increased reliance on insurance to transfer some of their risk, and this year's survey reveals the largest percentage of respondents ever to carry cyber insurance. Seventy-eight percent of respondents have cyber coverage, either through a standalone policy (55 percent), coverage blended with their professional liability program (13 percent), or as part of another policy or program (five percent). Just 12 percent do not buy cyber insurance and nine percent said they didn't know if they were covered for cyber risks.

TEN-YEAR CYBER INSURANCE PURCHASING TREND



For those organizations that still do not buy cyber coverage, price is the main issue – but this isn't merely a case of sticker shock. Commenters say they do not feel it is priced appropriately for their organization's risk or they cannot see the value for their organizations.

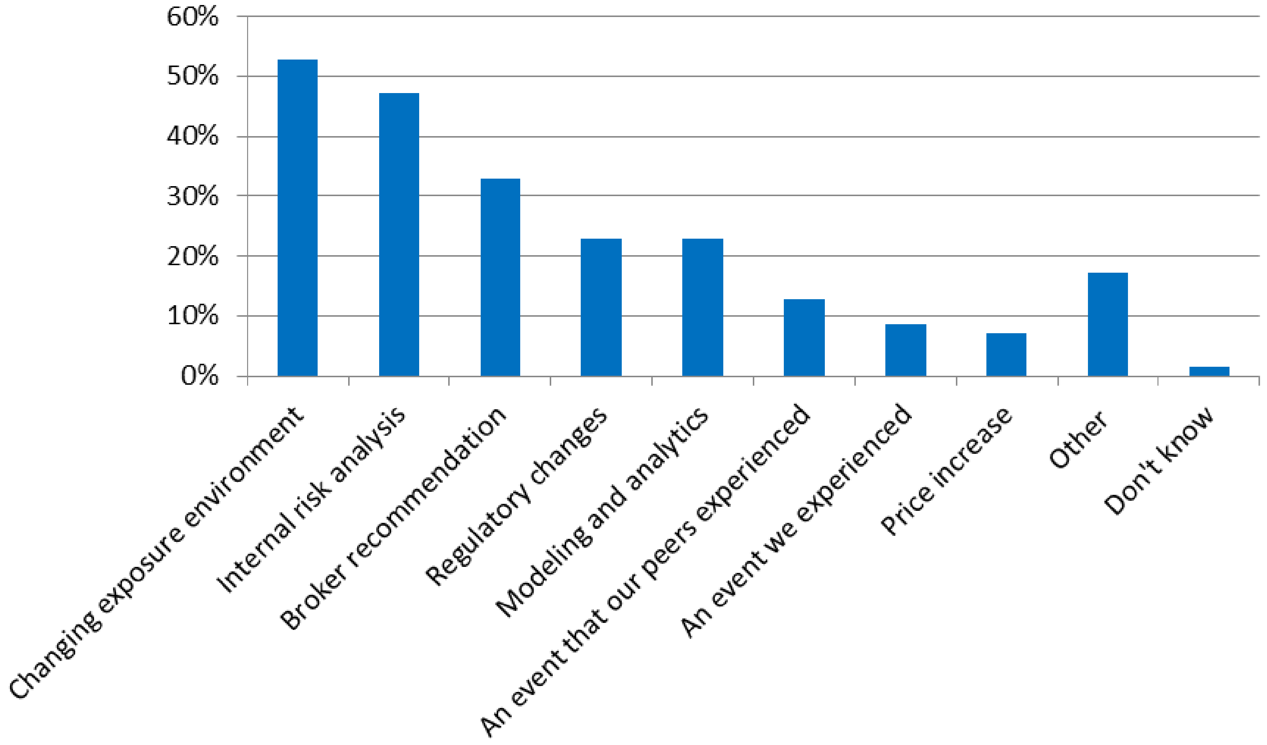
While 74 percent of non-buyers have considered the coverage, 21 percent have not – a few respondents said they are in the process of buying it. Internal struggles exist for some risk managers: one respondent said, "I cannot get my IT group to focus on the need and/or to see the risk transfer value of the insurance product."

Most respondents in this year's survey first bought cyber insurance in 2015, with 2017 being another big year for market growth. For five percent of respondents, 2020 marked the first year they bought cyber coverage. Additionally, it is interesting to note there were a few early adopters of cyber insurance in this year's survey, with 35 percent of respondents dating back to pre-2010 and four respondents buying cyber coverage before 2000.

Despite most respondents to last year's survey indicating they wanted higher limits and broader coverage on their next renewal, 60 percent of respondents to this year's survey said they made no changes to the structure of their programs. The cyber insurance market shows signs of changing, with tougher underwriting and pricing increases. In the past, respondents to this survey have indicated they bought more coverages and higher limits because the price was right, i.e., low. Now, rates are increasing substantially, and when buyers boost their limits and add coverages, it can be taken as a sign they value the coverage and need the protection. Cyber insurance is no longer a luxury item, even amid a hardening overall insurance market.

For those respondents who did change their programs, over half (53 percent) said they did so in response to the changing exposures or — in another sign of increasing sophistication on cyber risk — in response to internal risk analysis (47 percent). The most common changes were to add coverages (80 percent) and increase limits (71 percent), although 16 percent of respondents who changed their programs boosted their own retentions. These factors all point to a buying audience, and market, that has a better handle on the cost of risk.

FOR WHAT REASONS DID YOU CHANGE THE STRUCTURE OF YOUR CYBER INSURANCE PROGRAM?

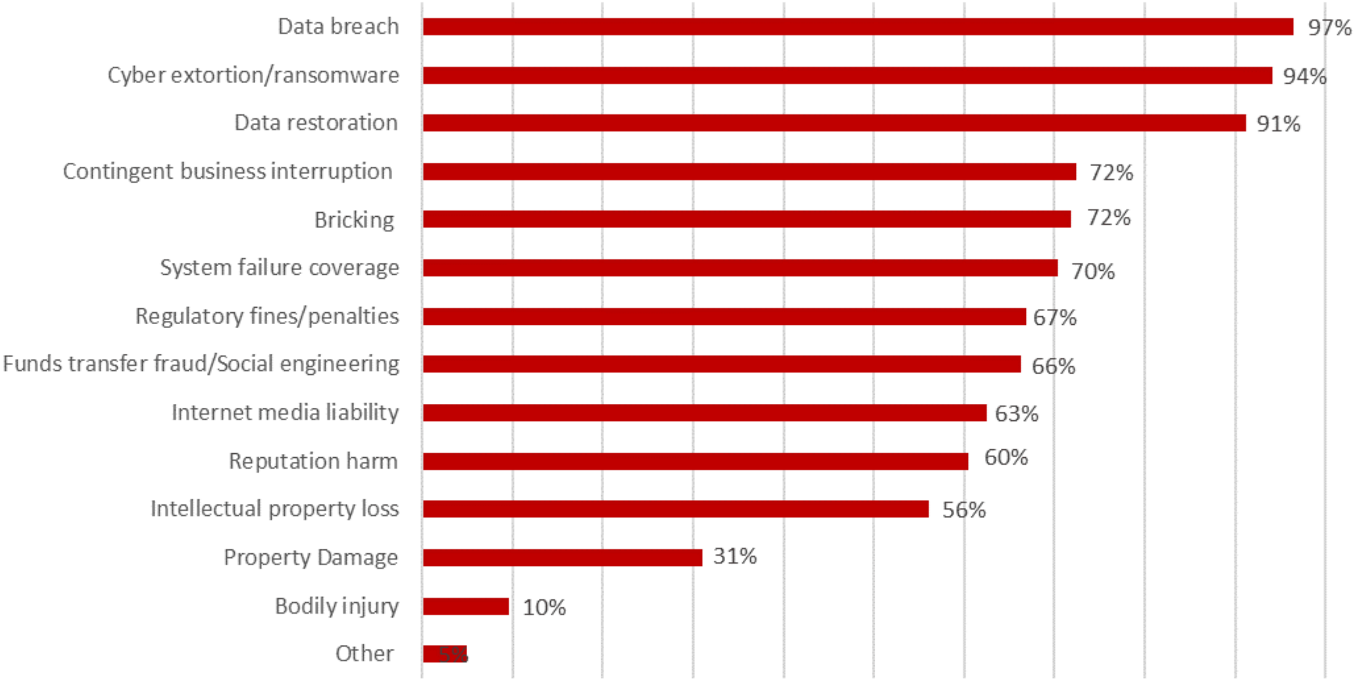


However, most buyers (60 percent) responding to the survey still rely significantly on recommendations from brokers and underwriters in the design of their cyber insurance programs. Less than a quarter (24 percent) are "heavily involved" in the crafting of policy language and 22 percent say they buy an off-the-shelf policy and add endorsements to meet their needs.

What's in a Policy?

As cyber coverage broadened in response to evolving risks in recent years, buyers have come to have high expectations for their cyber insurance. Data breach is the number-one most expected coverage for 97 percent of respondents, but respondents also recognize the need for cyber extortion/ransomware (94 percent), followed by data restoration (91 percent). Data breach coverage has remained steady as the top pick, but cyber extortion and data restoration have both risen in priority since last year.

WHAT DO YOU EXPECT A CYBER INSURANCE POLICY TO COVER?



The survey shows high interest from 72 percent of respondents in coverage for "bricking," i.e., when an electronic device becomes unusable following a cyberattack, but only 31 percent expect their policies to cover property damage. Bricking, as an element of cyber-related property damage, has become fairly standard in the cyber insurance market, but buyers need to know to look for it and ask their brokers to procure it.

Other coverages proved nearly as popular. Respondents said they expected their policies to cover contingent business interruption (72 percent) and system failure coverage (70 percent), funds transfer fraud/social engineering (66 percent), internet media liability (63 percent) and reputational harm (60 percent).

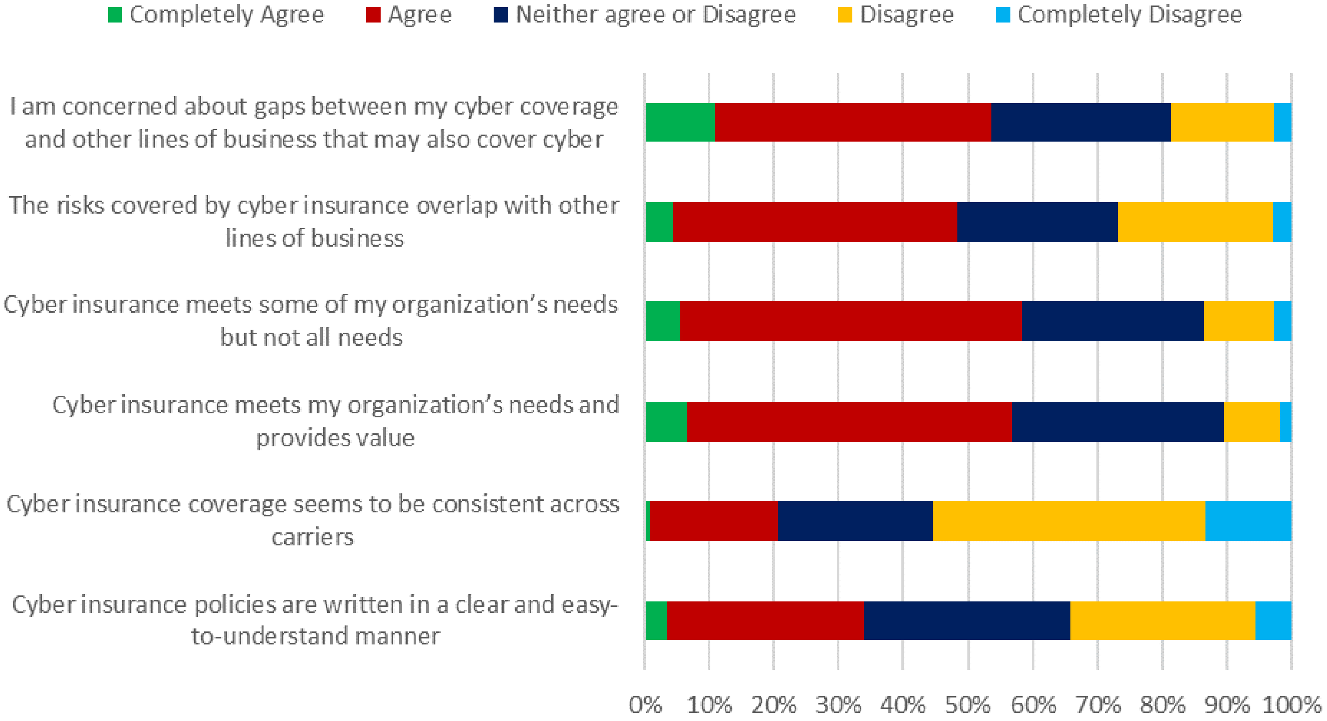
Internet media liability and reputational harm have both increased significantly as areas of concern for buyers this year. With this level of interest, these are conversations that brokers should be having with the clients about coverages.

The expectation that regulatory fines and penalties will be covered has dropped slightly (67 percent), and regulatory impact/uncertainty also fell as a reason for buying cyber coverage (30 percent, down from 35 percent last year). This may be a product of lack of significant fines and penalties under the European Union's General Data Protection Regulation (GDPR), but buyers and their insurance partners should still pay close attention to future developments with the California Consumer Privacy Act (CCPA), Illinois' Biometric Information Privacy Act (BIPA), and expanded privacy rules coming from New York financial service regulators.

Perspectives on Insurance

Though cyber insurance policies are still not considered "clear and easy to understand," this year's results show buyers getting a better handle on cyber insurance policies. The number of respondents who either "completely disagree/disagree" with the statement "Cyber insurance policies are written in a clear and easy-to-understand manner" has dropped: 34 percent this year compared to over 40 percent last year. Cyber insurance buyers are either getting the hang of policy wordings or policies have become more streamlined.

PLEASE ANSWER THE FOLLOWING:



However, since 55 percent of respondents still "completely disagree/disagree" with the statement: "Cyber insurance coverage seems to be consistent across carriers" it is unlikely greater standardization across insurers contributed significantly to the greater understanding. And, as noted, this is a group of cyber insurance buyers with five-plus years of experience with the coverage who are more likely to understand the definitions and provisions and can more easily compare and contrast between policies. The same may not be true for all buyers, or those new to the market, so it is still incumbent upon brokers and agents to guide their clients through the process.

The insurance industry also still has ground to cover in terms of clearly delineating where cyber risk should be covered. Just over a quarter of respondents (26 percent) feel cyber insurance does not overlap with other lines of business; 48 percent agree/completely agree it does. Another quarter (25 percent) neither agree nor disagree. However, a majority (54 percent) are concerned about gaps between their cyber insurance and other lines that may offer some cyber cover.

Even with continued variation on policy language, respondents feel they can identify both the value of their cyber insurance and the areas where it either falls short or creates conflict with other lines of insurance. More than half (57 percent) either agree or completely agree with the statement, "Cyber insurance meets my organization's needs and provides value," while 59 percent agree or completely agree with "Cyber insurance meets some of my organization's needs but not all."

With an eye toward meeting all needs, respondents have some thoughts on how they would like to see cyber insurance evolve in the future.

With an eye toward meeting all needs, respondents have some thoughts on how they would like to see cyber insurance evolve in the future. One commenter said, "It would be nice to consider a holistic policy with a draw-down for limits for specific coverage, much like auto. A 'combined single limit' approach. This will not be well received by insurers but think it something to consider…if priced correctly."

Another added, "I wish they would make a standard policy with all insurers to include full limits for social engineering, bricking and reputational harm. I believe the insureds would purchase these policies."

Respondents also see the underwriting process as helpful for identifying risks within an organization, with one commenter noting, "Insurers are asking a lot more questions and challenging our cyber security staff. This is good."

Cyber Events and Claims

Experiencing a cyber event, while unfortunate, may be the best test of a cyber insurance program and organizational cyber security preparedness. More respondents than ever before (31 percent) have experienced a cyber event that led to a business disruption or an economic loss, and of those, 51 percent filed a claim under their cyber insurance policies. For 74 percent of claimants, cyber insurance — either a standalone policy or a cyber endorsement — covered the claim. Another 11 percent reported the claims process is ongoing, but these results build upon and exceed our findings from last year's survey that cyber insurance pays covered claims.

Well over half of the respondents who filed a cyber claim (64 percent) were either "very satisfied" or "satisfied" with the outcome of the claims process. One respondent noted, "Our insurance carrier stepped in quickly and assigned our company to cyber legal and cyber terrorist specialists. I would have been lost without them."

However, another nine percent were "somewhat satisfied" and 12 percent were some level of dissatisfied, so the cyber insurance industry should not rest easy. Several survey respondents registered disappointment with aspects of the claims process and paying attention to concerns can improve the experience for all. In this and in previous surveys, respondents frequently cite claims falling below the deductible as their reason for dissatisfaction. Identifying appropriate retentions during the buying process should be a priority for all brokers and buyers. One commenter said, “The loss was not large enough to involve the insurance company’s legal counsel, so we were left to figure things out on our own.” Another noted, “Reasonably satisfied, although the coverage didn’t include everything we expected it to cover.”

“Very Prepared” for Breaches

Given respondents’ view that business interruption and reputational harm would be the worst outcomes of a ransomware event, it makes sense that organizations would focus on prevention and recovery. While protecting corporate reputation has been cited in past surveys as a reason to buy cyber coverage, this year’s survey shows new recognition that high-profile cyber events can have a lasting impact on customer goodwill.

As befits an audience that takes cyber risk seriously, respondents show high confidence on their levels of preparedness for cyber events. Sixty percent feel either “extremely prepared” or “prepared” to respond to a ransomware event, while 33 percent feel “somewhat prepared.” For insurers and brokers, the next step should be to assess how their clients define “extremely prepared” for a ransomware event. Just over the last year, ransomware as a threat has evolved to not only encrypting systems and demanding payment, but also exfiltrating data as leverage. Attacks against government entities, educational institutions, and healthcare organizations have become even more prevalent and successful and smaller and middle market organizations may be particularly vulnerable. [See sidebar on ransomware preparation]

Well under half the respondents (37 percent) are aware of value-added services/vendor panels offered by many cyber insurers, but they have not used them either pre- or post-breach. While this statistic makes sense for post-breach services, given the relatively few claims reported by respondents, this seems like an area where more emphasis on pre-breach risk mitigation (especially

ARE YOU “EXTREMELY PREPARED” FOR RANSOMWARE?

Back up your computers – Perform frequent backups of your system and other important files and verify backups regularly.

Store your backups separately – Make sure your backups are stored on secure, separate devices that are not accessible from your network.

Train your organization – Raise cyber security awareness among employees with regular training sessions.

Update and patch your computer – Ensure applications and operating systems have been updated with the latest patches.

Use caution with links and website addresses – Be careful when clicking directly on links in emails, even if the sender appears to be someone you know.

Open email attachments with caution – Be wary of opening email attachments, even from senders you know, particularly when attachments are compressed files or ZIP files.

Keep personal information safe – Check a website’s security to ensure the information you submit is encrypted before you provide it.

Verify email senders – If you are unsure whether an email is legitimate, try to verify the email’s legitimacy by contacting the sender directly. Do not click on any links in the email.

Increase your cyber risk knowledge – Stay informed about recent cyber security threats.

Use and maintain preventative software programs – Install antivirus software, firewalls, and email filters and keep them updated.

Source: CISA and Zurich North America Insurance considering some of the findings that organizations aren't training employees or assessing risk more frequently than annually) could be useful.

Of the 28 percent who had used the services, just under half (48 percent) said their needs were met. For 45 percent of respondents, vendor panels could be improved. One commenter said, "We have existing partners which often exceed panel vendors. Most panel vendors are aimed at immature organizations IMHO." Others reported that services need to be tailored to their individual risks and regulations to really demonstrate value. Others would prefer to use their existing partners. As one commenter noted, "The panel offerings are often undersized / not capable of responding to major events in a large multi-national organization, and the time to get them up to speed on the organization's systems and processes is not timely versus the use of pre-selected and on-boarded vendors of the insured's choosing."

The Impact of COVID-19

Any cyber risk management survey conducted this year would be incomplete without discussing the impact of the COVID-19 pandemic on the state of cyber security for organizations. Working remotely has inspired a lot of fear for risk managers, especially given the "human element" already discussed in this paper. With employees away from the routines and security restrictions of their physical offices, organizations feel less control over endpoints, networks, and device security. Organizations worry about phishing emails, business email compromise, data loss, and complacency that leads to carelessness. One respondent noted there is "not enough space to list all the risks."

On the other hand, one respondent said, "We feel pretty well controlled using VPN, pushing security updates regularly, and continuing employee education."

With employees away from the routines and security restrictions of their physical offices, organizations feel less control over endpoints, networks, and device security.

There may be a disconnect between the IT department and risk managers/insurance buyers on this new area of cyber risk, albeit a small one. While 63 percent of respondents said that they were either "very involved" or "somewhat involved" in assessing the risks of employees working from home, 36 percent said they are "not at all involved." Greater coordination between risk managers and the IT department, as with so many cyber-related topics, could only strengthen an organization's defenses by identifying more potential exposures.

Despite the obvious concerns, over half of respondents (54 percent) said that COVID-19 has not affected their view of cyber risk for their organization. Comments from respondents illustrate this divide. While many organizations feel they are facing the same cyber risks they would in non-pandemic times, others worry remote working creates a broader attack surface and makes it more likely that cyber events will occur.

If there is any silver lining to the challenges, it may be to test the flexibility and resilience of organizational cyber response plans. As one respondent commented, "It has shown that remote work is more broadly possible and appropriate than previously thought but doing so exposes the attack surface for the organization, thereby making the risk of a breach/successful attack more likely."

A significant majority (81 percent) of respondents have not changed their cyber security spend due to COVID-19, which should be taken as a positive sign of organizations' commitment to cyber hygiene even in uncertain times. Taken with comments from the survey that many organizations already heavily invested in cyber security, this is promising evidence that the economic strife of the pandemic is not hitting cyber security budgets hard. Where changes were made, respondents reported, it was to increase cyber security investments in response to the heightened risk – another promising trend that highlights the fact that businesses understand addressing cyber risk is a priority.

Methodology

For 10 consecutive years, Zurich North America and Advisen Ltd. have collaborated on a survey designed to gain insight into the current state of and ongoing trends in cyber risk management and insurance.

Invitations to participate were distributed by email to risk managers, insurance buyers, and other risk professionals. The vast majority of respondents were from the United States (78 percent), followed by Europe (10 percent), North America outside the U.S. (six percent), and elsewhere (seven percent).

The survey was completed at least in part by 404 respondents. The majority classified themselves as either Chief Risk Manager/Head of Risk Management Department (32 percent), a member of the Risk Management Department (28 percent), Chief Information Security Officer/Chief Privacy Officer (four percent), Other Executive (CIO, CEO, CFO) (12 percent) or other risk professional engaged in the buying process (24 percent).

A variety of industries were represented. Finance, banking, and insurance had the highest representation, with 27 percent of the total. Other industries with significant representation included manufacturing (eight percent), healthcare (nine percent), technology (five percent), and educational institutions (five percent). The “other” category represented 14 percent of respondents, many of whom indicated they were from nonprofit organizations or restaurants.

Businesses of all sizes responded to this year’s survey. Firms with between $1 billion and $10 billion in revenue comprised 30 percent. Large businesses with more than $10 billion in revenue represented 16 percent, but the majority of respondents came from smaller and middle market companies (less than $1 billion in revenue) at 54 percent.

The information in this publication was compiled from sources believed to be reliable for informational purposes only. All sample policies and procedures herein should serve as a guideline, which you can use to create your own policies and procedures. We trust that you will customize these samples to reflect your own operations and believe that these samples may serve as a helpful platform for this endeavor. Any and all information contained herein is not intended to constitute advice (particularly not legal advice). Accordingly, persons requiring advice should consult independent advisors when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with this publication and sample policies and procedures, including any information, methods or safety suggestions contained herein. We undertake no obligation to publicly update or revise any of this information, whether to reflect new information, future developments, events or circumstances or otherwise. Moreover, the sponsors remind you that this cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be appropriate under the circumstances. The subject matter of this publication is not tied to any specific insurance product nor will adopting these policies and procedures ensure coverage under any insurance policy.