Information Security and Cyber Risk Management

October 2021

ZURICH

Advisen
A ZYWAVE COMPANY

Contents

3 Introduction

4 Survey Highlights

5 Perceptions of Risk

9 Ransomware in Focus

12 Perspectives on Insurance

15 Strong Adoption of Cyber Insurance

17 Building a Program in a Changing Market

17 Claims Experience and Satisfaction

18 Assessing the Pandemic's Impact

18 Methodology

Introduction

For much of the last two decades, the story of cyber insurance has been one of building awareness of risk, risk mitigation, and of the need for cyber insurance. Our 11th annual Information Security and Cyber Risk Management Survey makes clear the message has been heard: Over 83 percent of respondents now buy cyber insurance, with 66 percent carrying standalone cyber policies. The goal for risk managers and their insurance partners now becomes to move past awareness toward strengthening resilience against all cyber events.

The results indicate obvious areas of concern for respondents – ransomware has risen to the top of priority lists worldwide – but the challenge for many organizations remains: "How do you manage the unknown?"

Uncertainties around risk assessment and incident response join new consternation around the cyber world's most severe hard market to date. Triple-digit premium increases, vanishing capacity, shrinking coverage[1], and shifted expectations around baseline controls have joined long-term frustrations over inconsistent policy language to create a truly challenging renewal process for insurance buyers[2].

While many respondents expressed confidence in their preparation, it is by no means universal. Considering the current state of the insurance market, risk managers will find pre-breach mitigation planning and excellent cybersecurity controls to be mandatory for underwriters. This year's survey highlights a few areas where risk managers may be lagging – and where their insurance partners can offer education and support.

Fear of ransomware events reverberates through the responses to many of this year's questions. These concerns are justified to some degree, but organizations may be too focused on elements of cyber events that lie outside their control. They worry about the type of threat actor or the scope of an attack, rather than identifying and defending critical assets.

The results indicate obvious areas of concern for respondents – ransomware has risen to the top of priority lists worldwide – but the challenge for many organizations remains: "How do you manage the unknown?"

While ransomware may be the outcome organizations most fear, they run the risk of missing the forest for the trees in this case. Ransomware may be one result, but the causes are almost always lax cybersecurity controls, failure to address known vulnerabilities, and poor planning. Rather than stressing about the unknowns, organizations will find their efforts better applied to analyzing and understanding their critical assets and operations, creating workarounds in the event of downtime, and identifying key vendors. Creating a high level of resilience allows risk managers and their organizations to keep the business going under any circumstances.

[1]While individual carriers have been consistent in their cyber coverage deployment, other markets have pulled back in coverage deployment by way of new exclusionary language. This term, and analogous terms in the remainder of the report, refer to the aforementioned general industry trend.

[2]Cyber policy forms are not yet standardized, since this is an emerging space. Because of this, product comparison for customers may be more difficult. This term, and others like it in the body of the report, refer to the aforementioned concept.

Survey Highlights

83 percent of respondents have cyber insurance—
the highest percentage to date in the 11 years of the survey.

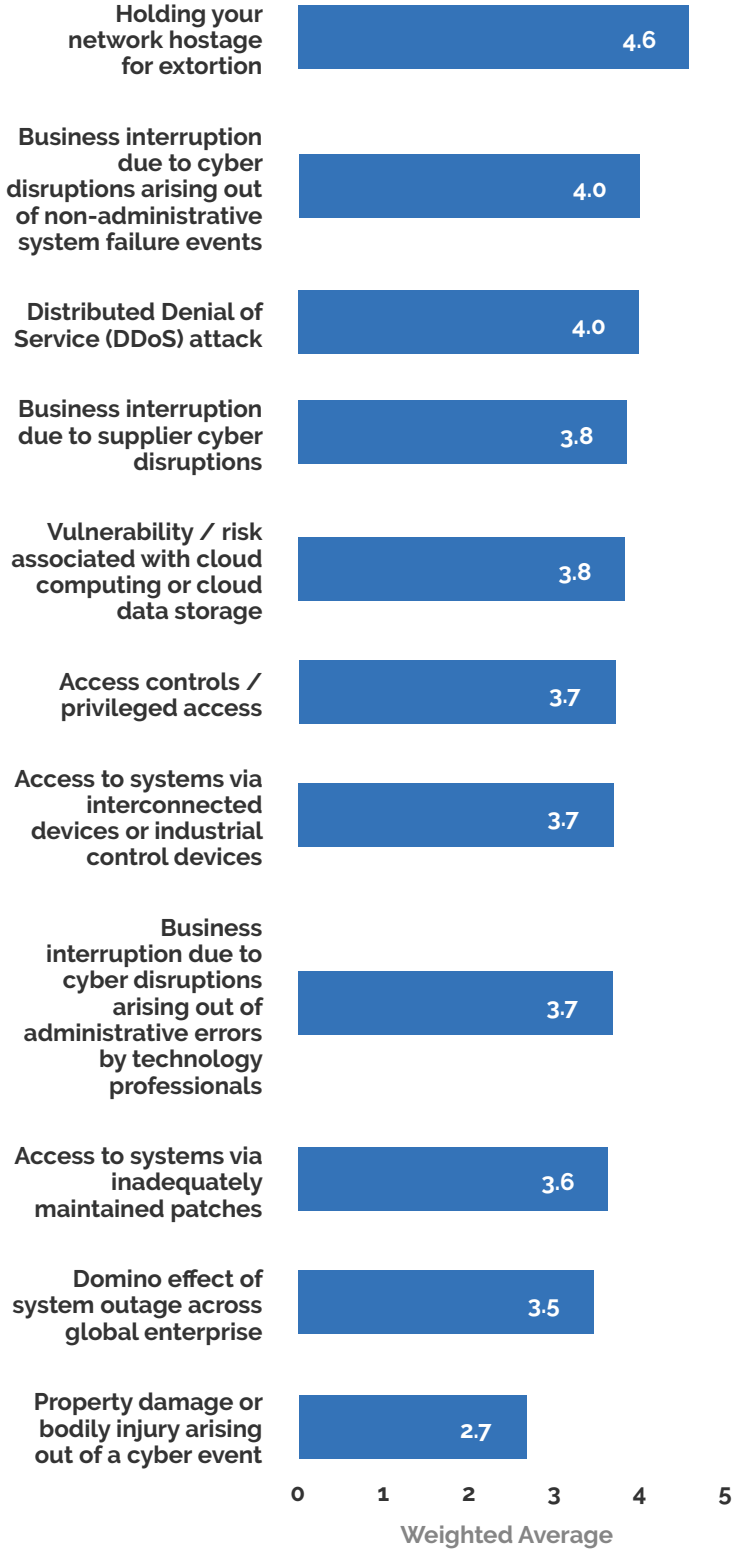
- 83 percent of respondents have cyber insurance – the highest percentage to date in the 11 years of the survey.
- For the first time, Cyber Extortion/Ransomware has pulled even with Data Breach, with 95 percent of respondents selecting it as a coverage they expect to be included in their policies. It was followed by Data Restoration at 90 percent; Business Interruption at 80 percent; and System Failure Coverage and Bricking at 73 percent.
- Risk managers may not be monitoring cyber threats to their organization frequently enough. The top response was "monthly" this year for 32 percent of respondents, followed by quarterly for 28 percent—underwriters will want to see more diligence from insureds.
- Results show that cyber risk management has significantly increased in priority to companies—86 percent say it is a significant concern and they've taken steps to assess their risk; and 65 percent have invested in cybersecurity solutions to mitigate risk and 61 percent say risk managers and IT work together to monitor risk.
- In terms of business continuity risks, respondents unsurprisingly ranked "Holding your network hostage for extortion" as the highest concern. However, business interruption due to technology failures or supplier cyber disruptions ranked much lower, indicating a possible blind spot for organizations.
- The hard cyber insurance market is hitting buyers on all fronts including retention, limits, price, and coverage. Respondent comments show significant worries about a "completely dislocated" market with triple-digit rate increases, shrinking coverages, and skepticism over whether insurers adequately analyze effective loss prevention measures.
- Buyers' frustration with the cyber insurance market's policy wording inconsistencies continues.
- The "unknowns" of ransomware may be the biggest issue for risk managers, with "we don't know what we don't know" a common complaint.

Perceptions of Risk

Organizations know they face a wide range of cyber risks to their data, their systems, and their business operations. This year's results show that cyber risk management has significantly increased in priority to companies – 86 percent say it is a significant concern and they've taken steps to assess their risk; and 65 percent have invested in cybersecurity solutions to mitigate risk and 61 percent say risk managers and IT work together to monitor risk.

Responses and comments both indicate a high degree of familiarity with potential threats and deliberation on the most pressing concerns for individual organizations. In terms of business continuity risks, respondents unsurprisingly ranked "Holding your network hostage for extortion" as the highest concern. Privacy violations were only deemed "high risk" by 29 percent of respondents, along with 23 percent of respondents viewing reputational damage due to privacy violation as high risk. Regulatory fines and penalties fell even lower in the rankings this year, with just nine percent deeming them a high risk .

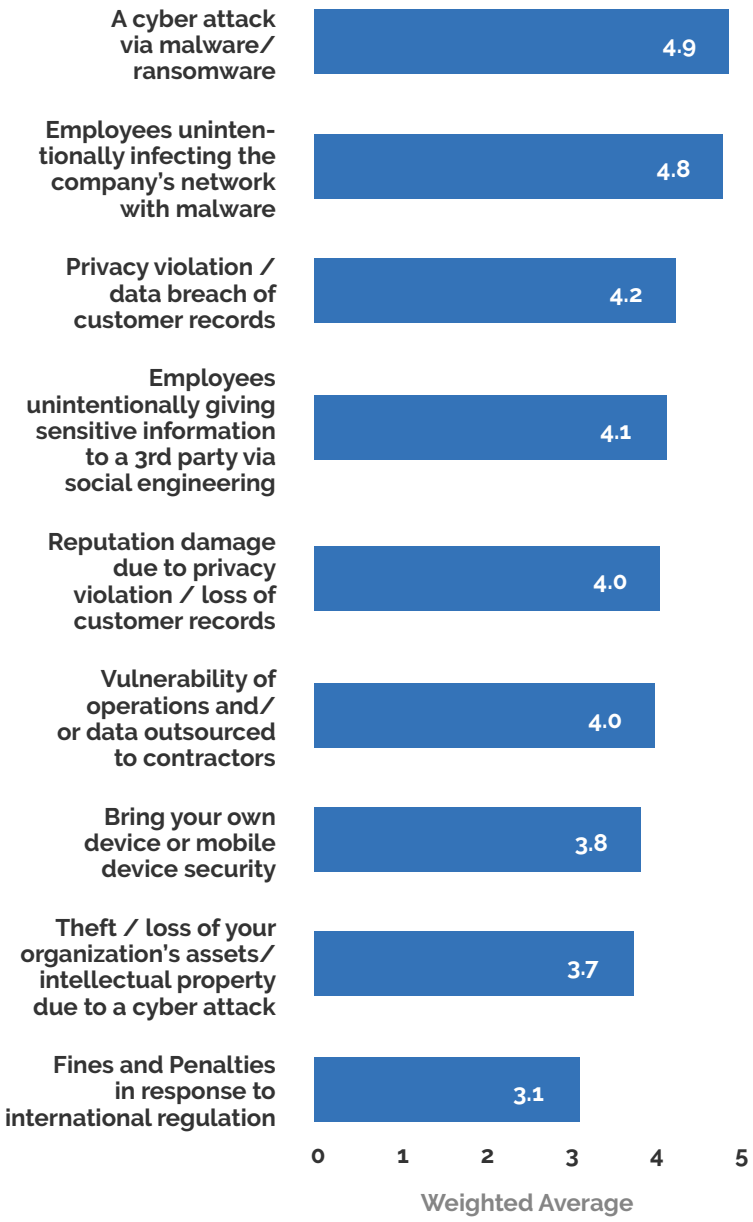
From the perspective of your organization, on a scale from one to six, please rate each of these business continuity risks



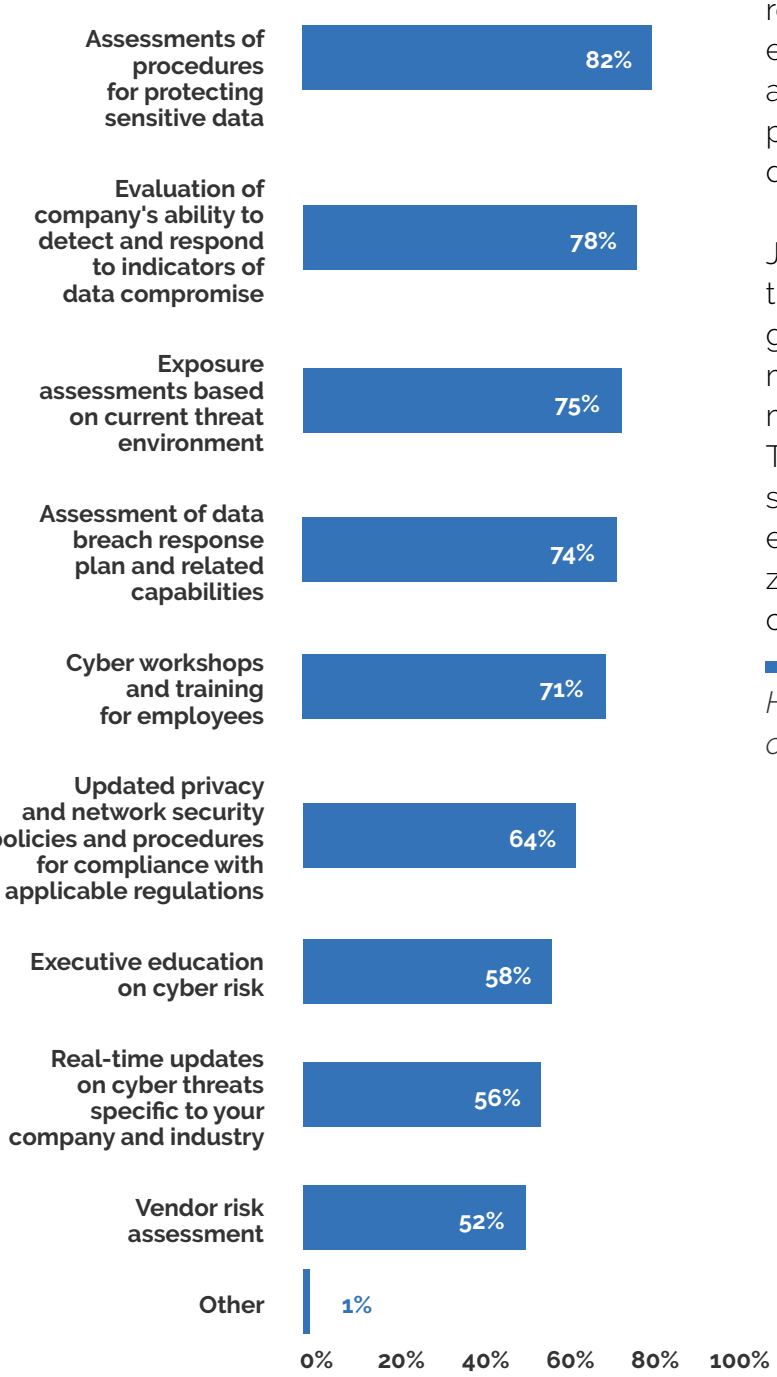
"Bring Your Own Device" security risk, which we highlighted as a concern last year due to work-from-home structures, remains second-lowest in terms of data integrity risks. However, "Employees unintentionally infecting the company's network with malware" ranks as a priority concern for business continuity risks, second only to ransomware. This suggests organizations may not be fully connecting improperly secured personal devices to the cyber intrusions that could give rise to business continuity and data integrity loss events.

With the high concern over employees introducing malware into digital environments, it makes sense that 71 percent of respondents offer training to employees (and 58 percent educate executives on cyber risk, a promising trend) – 30 percent offer training on an annual basis, followed by nearly a quarter that do quarterly trainings and 17 percent offering monthly education on cyber risks. The results show incremental progress from last year—when just nine percent offered monthly training—but with "Annually" still the most common answer and cyber threats evolving daily, organizations could decrease the amount of time between training opportunities to minimize or mitigate the risk of cyber events by keeping employees in the loop on threats.

From the perspective of your organization, on a scale from one to six, please rate each of these data integrity risks.



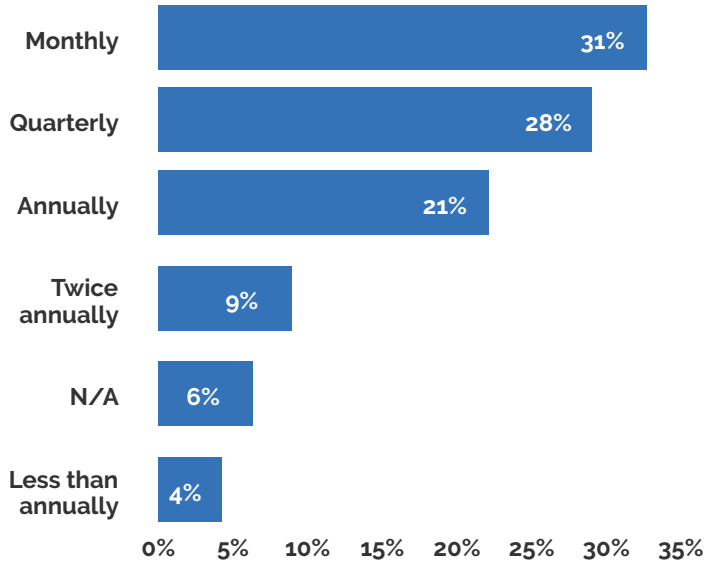
My organization's cyber risk management plans include the following.



Educational efforts represent just one aspect of the cyber risk management frameworks this year's respondents employ to prevent and mitigate cyber events. Results show a wide range of evaluations and protections, from exposure assessments and procedures to protect sensitive data to real-time updates tailored to specific companies and industries.

Just as organizations could be offering more regular training to employees, the survey showed potential gaps in threat assessment. Respondents were most likely to perform exposure assessments on a monthly (32 percent) or quarterly (28 percent) basis. This marks some slight progress from last year's survey but in today's fast-changing environment, even monthly threat assessments will leave organizations ill-prepared for both threat actors and their cyber insurance renewals.

How often do you assess your company's exposure to cyber risks based on the current threat environment?

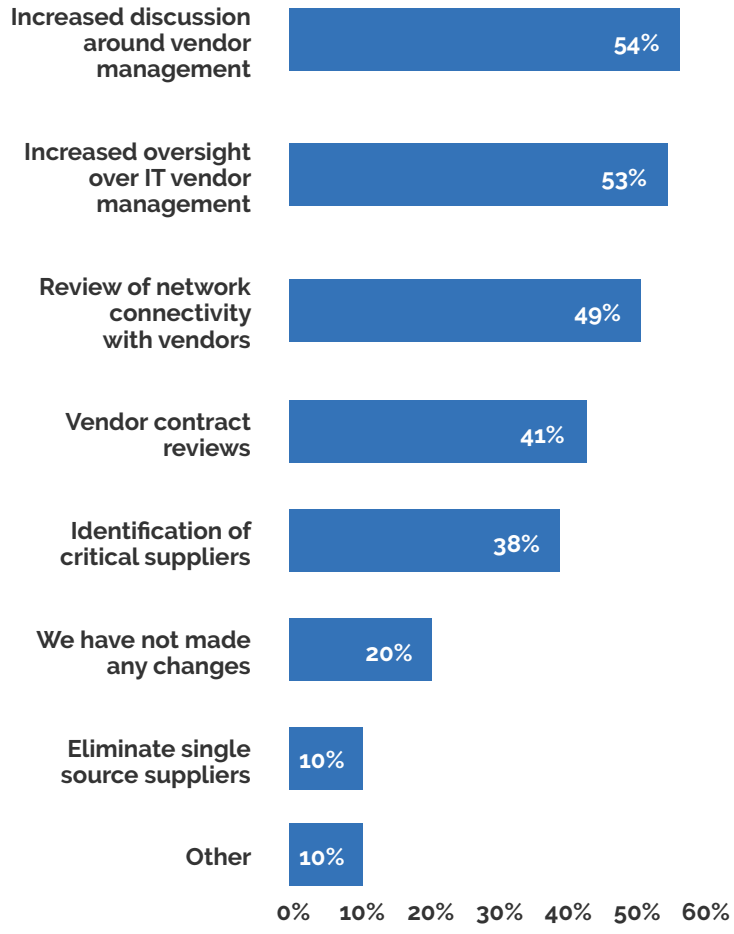


In today's fast-changing environment, even monthly threat assessments will leave organizations ill-prepared for both threat actors and their cyber insurance renewals.

However, vendor risk assessment ranks lower than all other facets of risk mitigation planning (just 52 percent of respondents selected it as part of their plan). Business interruption due to technology failures or supplier cyber disruptions also ranks lower on a list of business continuity concerns, with respondents more likely to view these as moderate concerns. With cybercriminals increasingly leveraging third-party vendors to launch attacks on a broader scale, companies should be forewarned vendor risk is not an area to ignore. As an example, for this year's survey, we asked whether organizations made any changes as a result of recent high-profile cyber supply chain events, such as SolarWinds. Just over half (54 percent) reported "increased discussion around vendor management" or "increased oversight over IT vendor management" (52 percent). While this is a positive step, far fewer (38 percent) took the next logical step of identifying critical suppliers or eliminate single-source suppliers (10 percent). Respondents cited exploring higher cyber insurance limits in response – an option that would transfer more risk but not ultimately address the source of the risk.

That said, the message that backups can save the day has been received for a majority of respondents —73 percent perform daily backups. Comments indicate that many organizations are backing up mission critical systems automatically or every five to 15 minutes. This statistic highlights the significant increase in sophistication of this year's responders. Greater frequency, along with additional methods of protecting backups—whether through encryption or air-gapping systems—can further mitigate business interruption and/or ransomware exposure.

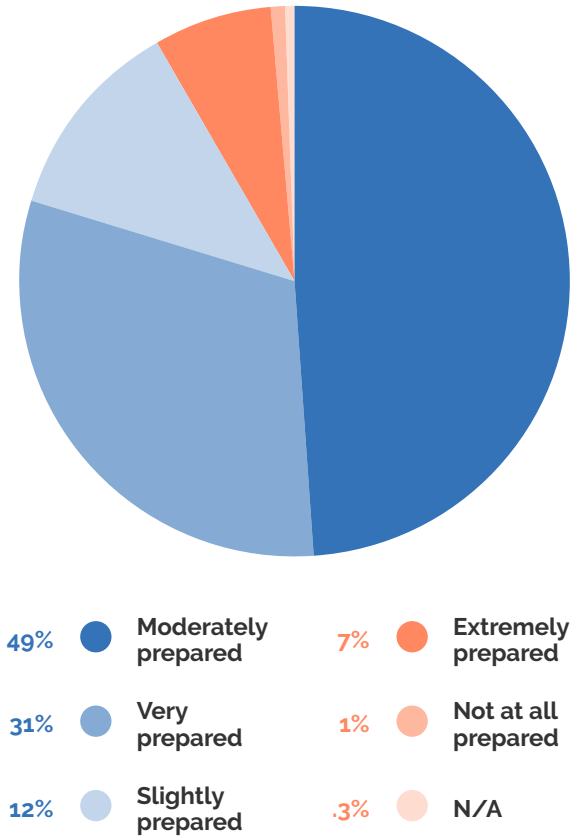
What, if any, changes has your organization made as a result of recent high-profile cyber supply chain events?



Ransomware in Focus

For the first time, the survey featured questions specific to ransomware, a timely inclusion given the rising frequency and severity of events. Responses demonstrate a keen awareness of ransomware as a potentially existential threat, and cautious confidence in their preparedness.

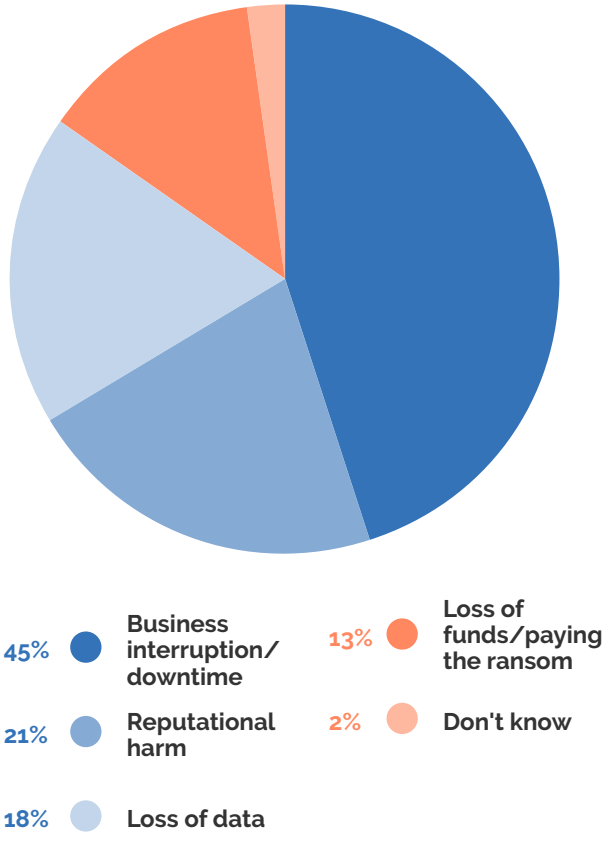
How prepared do you feel your organization is to respond to a ransomware event?



This year's respondents have plenty to say about ransomware—they know it has become the most common form of cyber event and want to avoid it any way possible. A significant majority of respondents (80 percent) say they feel "very prepared" or "moderately prepared" to face a ransomware event. Another seven percent go so far as to describe themselves as "extremely prepared."

The comments offer a closer look at how organizations view ransomware prep – several say they faced no challenges and feel prepared; others worry about educating their employees effectively or keeping pace with sophisticated, dedicated hackers. It's important to remember this year's respondents represent an exceptionally cyber-savvy group; organizations facing cyber threats these days are more likely to feel less well-prepared.

In your view, what would be the worst outcome of a ransomware event?



However, respondents also worry that no matter how much they prepare, it will not be enough to fully overcome a ransomware attack. They have identified their biggest concern – the focus on business interruption persisted through our ransomware section, with 45 percent of respondents citing it as the worst outcome of a ransomware event, followed by reputational harm as a distant second at 21 percent. Loss of data and loss of funds/paying a ransom came in even lower on the list of ransomware consequences.

Ransomware preparedness challenges for organizations primarily relate to resources and time – 30 percent of respondents say they do not have the resources to prepare, while 15 percent do not know how to start preparing. Another 15 percent said they do not have buy-in from senior management.

Check out this resource for additional information on how to get started.

"It's hard to keep up with the evolving ransomware approaches. Previously, it was simply an encryption of data, now the challenge is the exfiltration of private data and the potential OFAC/OSFI/HM Treasury restrictions on paying ransoms to certain threat actors," said one commenter.

The "unknowns" of ransomware may be the biggest issue organizations face. Two comments sum up many of the reservations: "We have a blueprint plan but until it happens no one knows how effective it will be" and "While our Cyber Risk Security efforts seem very robust, it's difficult to know what we don't know."

Another commenter noted gloomily, "Too many threat vectors to protect," while another said "There are no fail-safe preparations."

The above comments make even more sense taken in context with the fact that 76 percent of respondents have not experienced a ransomware event; seven percent said they did not know if their firms had experienced events.

Of the 17 percent of respondents who experienced a ransomware attack, 60 percent did not pay a ransom and rebuilt their systems from backups; only 10 percent did not pay and lost data. Just over a quarter (27 percent) paid ransom and regained access to their system; no respondents paid and lost data or failed to regain access. In terms of insurance coverage for ransomware claims, 47 percent had their claims covered by their cyber policy and 49 percent did not file a claim.

Two comments sum up many of the reservations: "We have a blueprint plan but until it happens no one knows how effective it will be" and "While our Cyber Risk Security efforts seem very robust, it's difficult to know what we don't know."

Several ransomware victims said they felt experiencing the event helped refine their cybersecurity controls for the future. Many commenters highlighted the value of tabletop exercises in testing their incident response plans; this could aid in boosting the confidence level of all organizations on ransomware and beyond.

Perspectives on Insurance

With ransomware top of mind for most organizations, buyers' expectations for coverage have evolved accordingly in this year's survey. For the first time, Cyber Extortion/Ransomware has pulled even with Data Breach with 95 percent of respondents selecting it as a coverage they expect to be included in their policies.

While data breaches are still a concern, respondents have come to view any disruption in their ability to conduct business just as daunting as the compromise of data they hold.

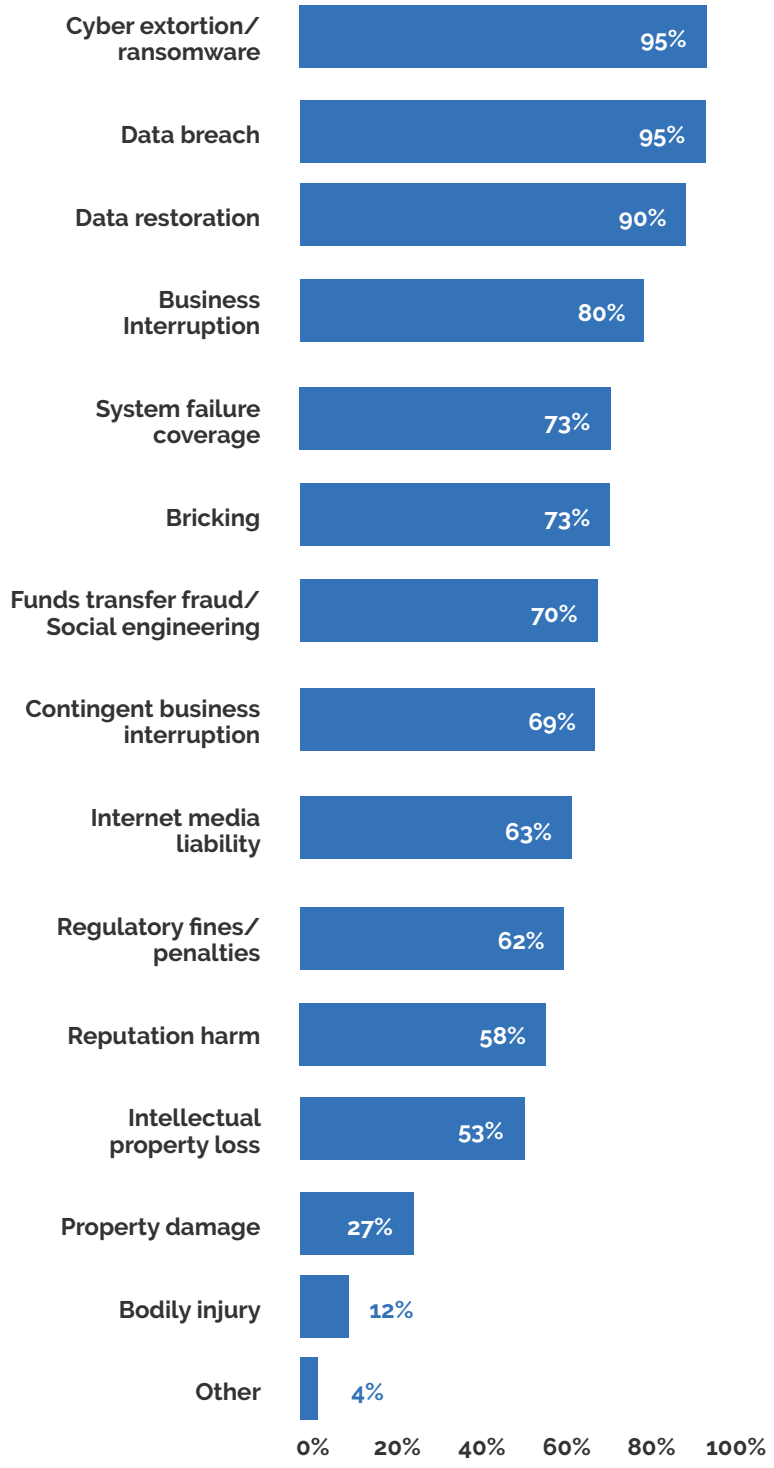
Coverage for Data Restoration came in third, with 90 percent of respondents selecting it; Business Interruption at 80 percent; and System Failure Coverage and Bricking at 73 percent. Nearly all coverage options were selected by at least half of the respondents, except bodily injury (12 percent) and property damage (27 percent).

Most respondents (78 percent) say their cyber policy covers cyber-related business interruption coverage, but fewer (still more than half at 55 percent) have cyber-related contingent business interruption cover.

Nearly a quarter (23 percent) said they do not know if their policy covers contingent business interruption cover; with the rising number of cyber events at third-party vendors, this is an action item for risk managers to ensure that they can continue operating in the event of a supply chain event.

As one commenter said, "I expect all of this; however, reality is different."

What do you expect a cyber insurance policy to cover?

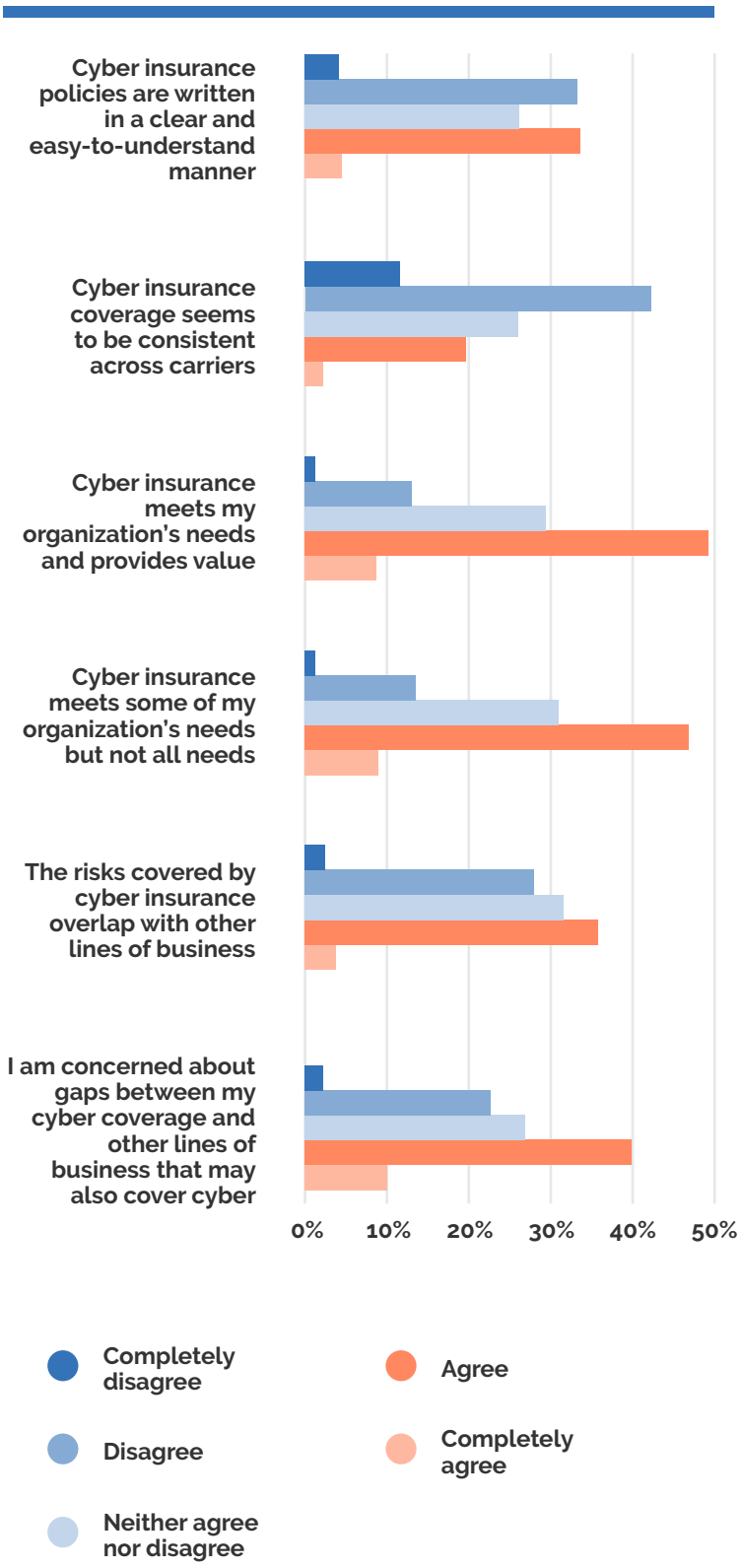


Respondents registered frustration with the ongoing hard insurance market, describing it as "completely dislocated." Commenters report triple-digit rate increases, cutbacks on coverage, and capacity constraints.

"Premiums have skyrocketed and applying for coverage is more extensive in the application realm," said one respondent, while another commented, "Massive list of subjectivities to bind coverage. The network upgrades are significantly more expensive than the needed coverage even with the 300 to 400 percent increases in annual premium."

Comments also reflect consternation over the cyber insurance market's policy wording inconsistencies and multiple commenters throughout the survey still feel the market has not truly matured. However, the demand for better cybersecurity controls and heightened risk evaluation reflect the market's intent to zero in on the factors that most impact underwriting and pricing.

Amid a hard market, no ground has been gained on the long-term question of whether cyber insurance policies are written in a clear and easy-to-understand manner – 37 percent of respondent still "disagree/completely disagree" with this statement, up from 34 percent in 2020, but still slightly lower than 40 percent in 2019. On the other side, another 37 percent "agree/completely agree" with the statement and 26 percent neither agree nor disagree.



Consistency across the industry on coverage has barely budged between 2020 and 2021 – 54 percent of respondents disagree or completely disagree that coverage has become standardized across carriers. However, a challenging cyber insurance market with highly varied appetites for risk may not create an environment conducive to consistency. Insurers have restricted different aspects of coverage based on their own loss experience, accelerating the inconsistency trend and creating further confusion.

Some slow-but-steady progress seems to have been made in reducing gaps between cyber coverage and other lines of business that may also cover cyber – 49 percent of respondents say this concerns them, down from 54 percent in 2020 and 39 percent say they see overlaps in coverage (down from 48 percent last year).

A significant percentage of respondents in both questions neither agree nor disagree on gaps (26 percent) or overlaps (31 percent) – this seems high for an issue with potentially severe consequences for not having the right coverage. Are there overlaps, but risk managers have grown accustomed to them? Have the industry's non-affirmative cyber actions/ responses provided enough affirmative coverage to eliminate the most pressing concerns? Comments from the survey participants suggest insurance buyers have found ways to achieve coverage certainty; for example, placing cyber and crime coverage with the same carrier to avoid disputes.

However, despite these issues, more than 57 percent of respondents agree with the statement, "cyber insurance meets my organizations needs and provides value," while 55 percent believe it meets some but not all of their organization's needs. These results are close to unchanged year-over-year, and may indicate either intangible cyber risks, or an understanding that risk transfer must be accompanied by a range of cyber risk management tools. It may also reflect the level of sophistication of our respondents – policies are not consistent, but savvy buyers now understand what to look for to meet their organizations' needs.

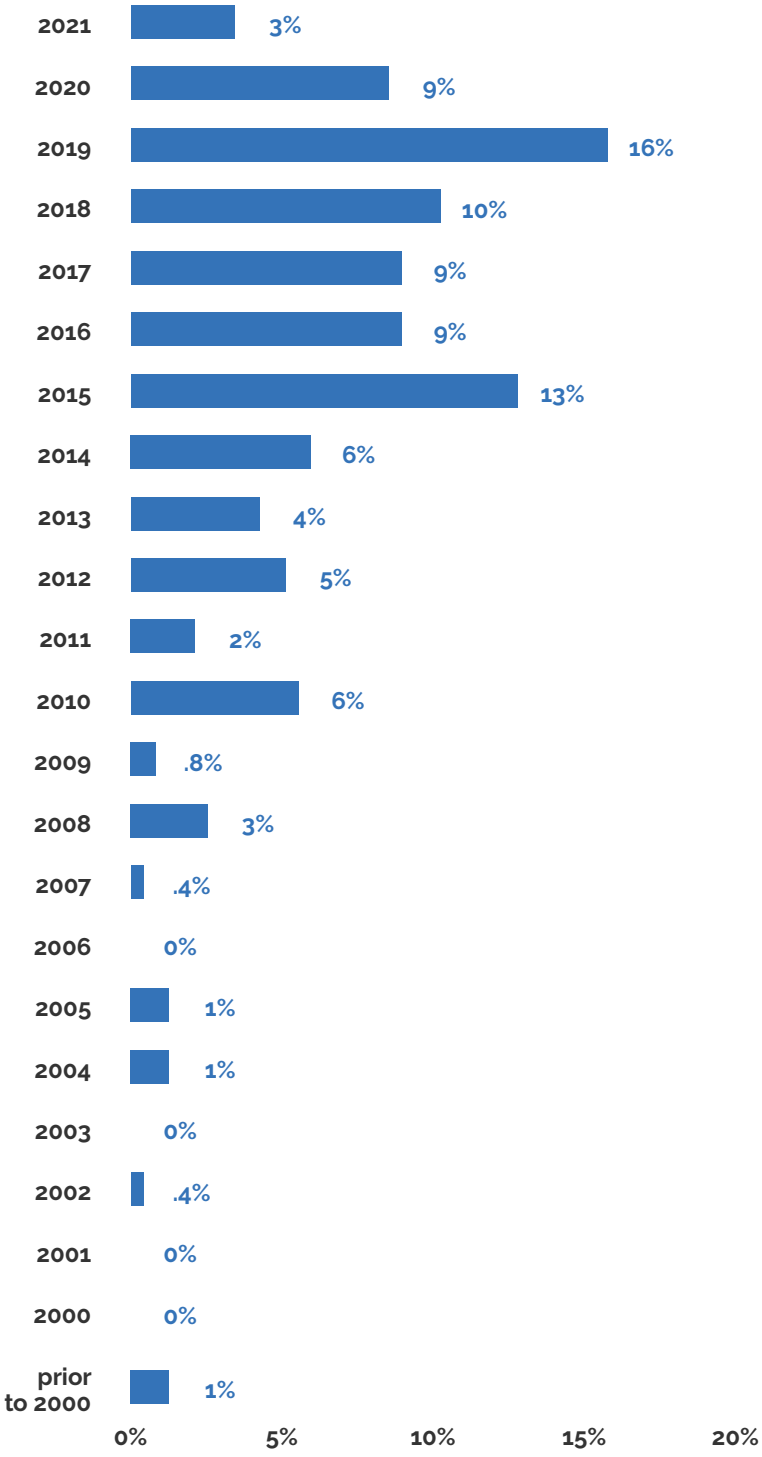
Strong Adoption of Cyber Insurance

The importance of cyber insurance as part of a comprehensive risk management program is clear in the fact that 83 percent of respondents carry the coverage – the highest percentage to date in the 11 years of the survey. Buyers increasingly want dedicated coverage – 66 percent buy standalone cyber policies, up from 55 percent in the 2020 survey. Others have cyber coverage as an endorsement, blended with their professional liability program, or included with the purchase of a technology product, but there is a clear preference for standalone policies in this year's survey.

Just 11 percent do not carry the cover and five percent do not know if they do. Respondents that do not buy cite high cost (48 percent) and budget constraints (23 percent), but others cite their brokers' lack of discussion in their insurance renewal process or worries about limited coverage or denied claims. Others commenters discussed engaging in the cost-benefit analysis for cyber insurance, which may be even more of an obstacle in 2021 as rates spike and coverage becomes more conditional on costly security upgrades.

Given the digital upheaval associated with the COVID-19 pandemic, we were curious to see whether 2020 and 2021 drew a rush of new buyers to the cyber insurance market. For the respondents of this year's survey, however, 2019 was the big year for buying. The threat of ransomware may have been the biggest driver in 2019 to the present; news of major retail breach events drove purchasing in 2013-2015.

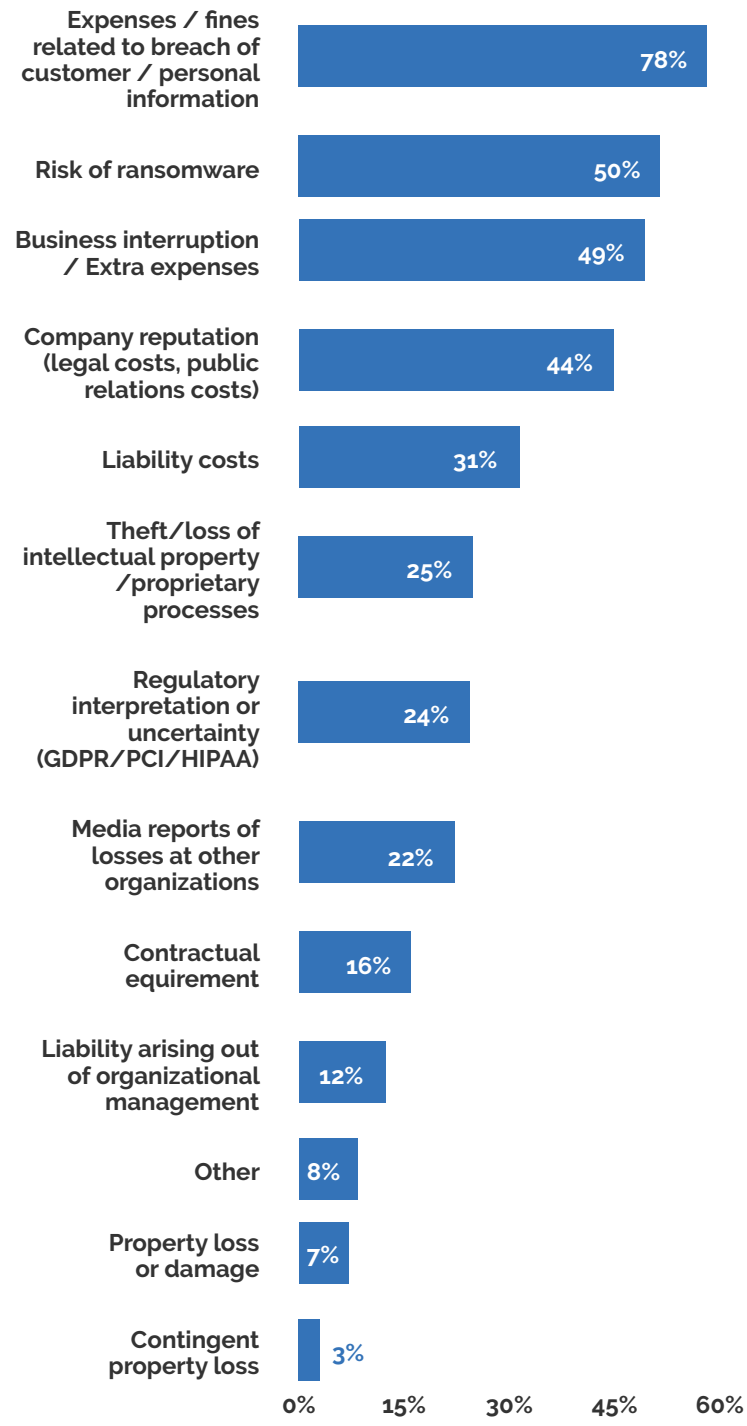
When did your firm first purchase cybersecurity and privacy coverage?



Expenses and fines related to breach of customer information remains the top reason to buy cyber coverage at 57 percent, but business interruption is close behind at 51 percent.

Risk of ransomware (50 percent) and reputational harm (44 percent) also ranked highly on the list of reasons to buy. Respondents cite access to technical expertise, reducing liability exposure for management, and "fear of the unknown" as the key reasons. The value of cyber insurance is assured since, as one respondent noted, "because we know better."

What were the primary reasons for purchasing this type of coverage?



Building a Program in a Changing Market

Survey responses demonstrate a commitment to maintaining cyber insurance programs with as much coverage as possible during a tough market cycle. The majority of respondents (62 percent) say they did not alter the structure of their cyber insurance program in the last year; but of those that did, many (65 percent) opted for higher limits, added coverages (39 percent), and increased retentions (39 percent).

Changes, per the comments in the survey, were not always voluntary but came as a mandate from carriers in response to ransomware, especially for increased retentions. Buyers also remain unconvinced that their premium prices and terms and conditions reflect the maturity of their organizations' cybersecurity programs.

> "I changed from one carrier to two carriers to maintain the same capacity, just with more layers. In the coming cyber renewal, I may need to introduce another layer as well, just to keep the same total limits."

As one commenter remarked, buyers are "struggling to find needed additional limits without material financial impacts … I know … good luck with that!"

Claims Experience and Satisfaction

In a statistic that speaks well of the cybersecurity posture of this year's survey participants, 70 percent of respondents have not experienced a cyber event of any kind. Of those that have, 18 percent have experienced a data breach, seven percent experienced a business interruption event, and five percent experienced an event that was both.

For the few respondents who experienced a cyber event and filed a claim, their standalone cyber insurance policy covered the loss (76 percent). Just over a quarter did not file a claim (27 percent), and nine percent had the claim covered under another type of policy endorsed to respond to cyber events.

Despite limited claims experience in the survey sample, most of the respondents who had a cyber claim paid were either "Satisfied" of "Very Satisfied" with claims handling (64 percent).

One respondent raised an excellent point: "It was a small claim that fell below the policy retention anyway, but served as a good test run for future, heavier losses."

A few comments illustrate dissatisfaction and offer insight into both insurers pressing for improved protocols for insureds and the need for planning out breach response ahead of time: "There was coverage for funds transfer fraud, but only if our employees follow all specific steps to verify the new account information. Apparently, because our employee did not call and get verbal confirmation from the vendor, that allowed the carrier to deny the claim." Another noted: "It was obvious that the adjuster and insurer did not understand our business and the strength of our IT department. Also, it was difficult to agree on breach coach or other support services."'

Even for organizations that have not experienced a cyberevent, any pre-breach planning should involve advance communication with cyber claims teams to understand how incident response will unfold.

Assessing the Pandemic's Impact

In 2020, survey respondents in this section faced cyber risk during a pandemic with a great deal of trepidation, with one respondent saying there is "not enough space to list all the risks." One year later, the risks that come along with remote work continue to be the biggest concern and time appears to have given respondents a better sense of the types of exposure they face, if not the ability to completely mitigate those risks. However, many respondents were already positioned for remote work but faced greater levels of phishing attempts.

Just 13 percent say the pandemic affected their view of risks "a great deal," while 28 percent said it impacted their perspective "a little." Over a quarter of respondents said it did not affect their view of the risk at all. This appears to be because even pre-pandemic, most risk managers saw cyber risk as a significant concern.

> The cyber insurance market can take heart in one commenter's view that "Cyber insurance remains a priority, with or without a pandemic."

Well over half (60 percent) of respondents have not changed their cyber-related investments or spend due to the pandemic; for those that did, they cite higher insurance costs and intentional budget increases to improve their systems.

And finally, the cyber insurance market can take heart in one commenter's view that "Cyber insurance remains a priority, with or without a pandemic."

Methodology

For 11 consecutive years, Zurich North America and Advisen, a Zywave company, have collaborated on a survey designed to gain insight into the current state and ongoing trends in cyber risk management. Invitations to participate were distributed by email to risk managers, insurance buyers, and other risk professionals.

The survey was completed at least in part by 386 respondents. The majority classified themselves as either Chief Risk Manager/Head of Risk Management Department (33 percent), a member of the Risk Management Department (22 percent), Chief Information Security Officer/Chief Privacy Officer (five percent), Other Executive (CIO, CEO, CFO) (19 percent) or other risk professional engaged in the buying process (21 percent).

A variety of industries were represented. Finance, banking and insurance had the highest representation, with 18 percent of the total. Other industries with significant representation included manufacturing (11 percent), construction (10 percent), professional services (eight percent), educational institutions (nine percent), and healthcare and technology (both six percent). The "other" category represented 13 percent of respondents, many of whom indicated they were from nonprofit organizations and a wide range of specialized industries.

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 10 percent, but the majority of respondents came from smaller and middle market companies (less than $1 billion in revenue) at 61 percent.