QBE

2024

Cyber Insurance Report

Introduction

In today's increasingly digital world, cyber insurance has become a must-have for businesses of all sizes. A recent survey of risk professionals and insurance buyers affirms that cyber insurance has achieved significant market infiltration, particularly by large companies. More than half the respondents were from large organizations, and over 80% carried some type of cyber coverage.

While the survey—a collaboration between QBE and Zywave—confirms that the risk management community understands the importance of transferring cyber risks to an insurance carrier, it also reveals that many companies fail to seize the full potential of their cyber insurance offerings. While many survey respondents said they are interested in the value-added risk management services in cyber policies—such as threat intelligence, claims acumen, guidance on preventive measures and privacy matters, among others—there is a low take-up rate of most of these features.

The survey suggests cyber insurers and brokers can more effectively communicate to enhance client risk resilience.

Key takeaways

Survey respondents commented that **risk transfer is the primary value of a cyber insurance policy,** with an insurer's breach response services (83%) and incident response planning and support (73%) not far behind.

50% of respondents were aware of additional risk management services offered by insurers. Approximately 40% of respondents took advantage of these risk services, indicating that **awareness was a key part of respondents taking advantage of the often complementary additional service offerings provided by insurers.** Many survey respondents expressed challenges regarding the cost of cybersecurity tools, resources and staffing. Value-added services like threat intelligence and preventive measures would help remedy these concerns. Better communications by brokers and insurers regarding the availability of risk management services could lead to a greater understanding of their respective benefits.

The survey findings indicate that **clients are interested in discussing cybersecurity, risk mitigation, industry trends, and other topics with insurers and brokers.** Industry professionals who communicate more effectively with clients to enhance their cyber awareness and education could generate a higher overall opinion of the value-added services offered by carriers.

The survey indicates an **opportunity to discuss such topics with directors and officers of companies**, especially at larger organizations, which make up the majority of the respondents. At present, insurers and brokers engage in discussions primarily with corporate risk managers, with 72% of respondents citing the role as the cyber risk purchasing decision-maker. Fewer than 4 in 10 chief information security officers, by contrast, are involved in the purchasing decision, despite their primary role leading cybersecurity.

A similar opportunity exists for insurers and brokers to **engage board members in discussions regarding cyber insurance risk transfer and related risk management and mitigation services**. Fewer than 1 in 5 boards of directors are familiar with the company's cyber insurance policy and related services. As boards become more engaged in their company's cyber risk management strategy, insurers and brokers can help flatten the learning curve.

Value of cyber insurance

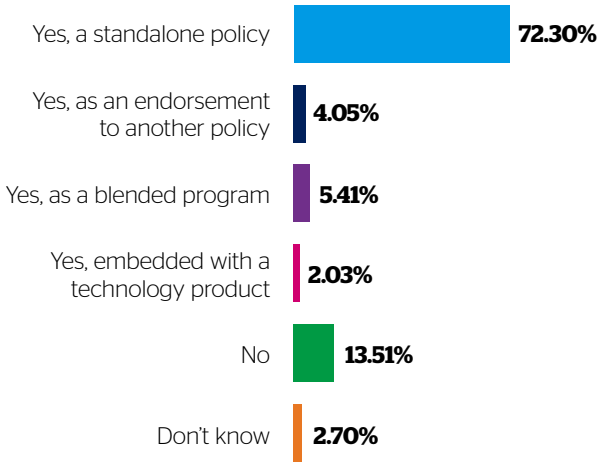
Over the years, risk professionals have come to understand the important role played by cyber insurance, igniting huge growth in the availability of cyber insurance and powering a substantial increase in the size of the cyber insurance market. The reason for this ample growth is the unique value of a product that protects companies against financial losses caused by cyberattacks—cyberattacks that impact applications, devices, networks and users, leading to data loss or compromise and significant business disruptions. The survey affirms this value.

More than **80%** of respondents (over half of them from large companies) buy some form of cyber risk transfer.

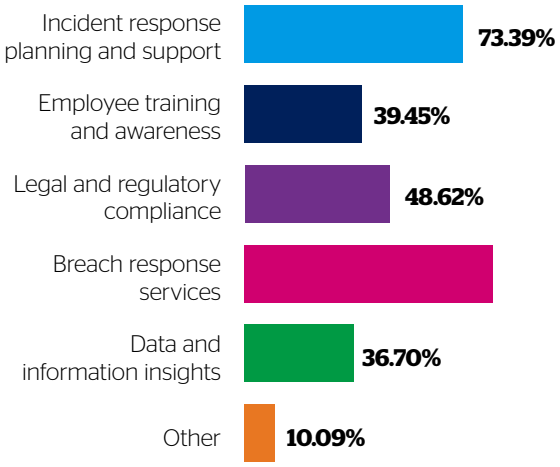
The price of the insurance policy appears to be less of a concern than in the past. Clients no longer perceive cost as a material barrier to purchasing cyber insurance. Overall, the price of cyber insurance ranked fourth in a survey question asking respondents about their challenges in managing organizational cyber risk. The cost of cybersecurity systems, services and the availability of qualified IT staff were cited as more pressing challenges.

A factor in the growth of the cyber insurance market and positive perceptions of its value is the relatively high rate of cyber incidents. More than 60% of survey respondents said they had experienced a cyber event, yet only 36% of the respondents filed a cyber claim. The remainder of respondents either hadn't purchased cyber insurance at the time of the event, or the related cost fell below the policy's deductible.

Do you currently purchase cyber insurance?



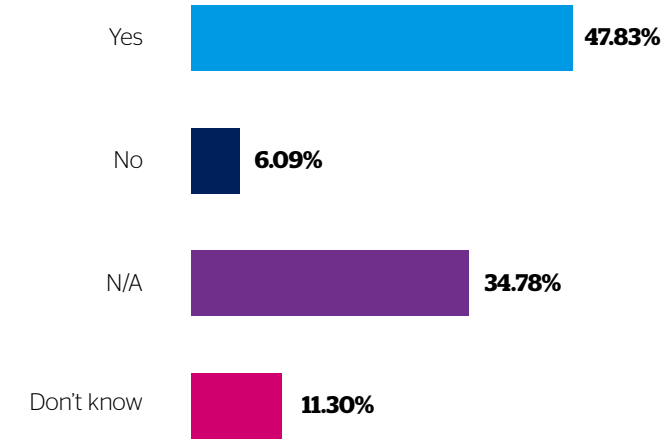
What do you view as the value of cyber insurance beyond risk transfer? Select all that apply.



Respondents who filed a claim on their cyber insurance policy describe their interactions with the insurer as largely positive. Nearly two-thirds (64%) of respondents said the insurer handled their claim quickly, efficiently and with an eye toward excellent service. The vast majority felt their carrier met their needs at a challenging time. The chief complaints by the survey respondents regarding the claims process were the length of the claim resolution process, a lack of communication and the tone of interactions.

Cyber incidents continue to occur at a relatively high rate. More than **60%** of the survey respondents said they had experienced a cyber event, yet only **36%** of the respondents filed a cyber claim.

Are your cyber carriers meeting your claims needs?



Have you ever experienced a cyber incident?

Medial take-up rate of cyber risk services

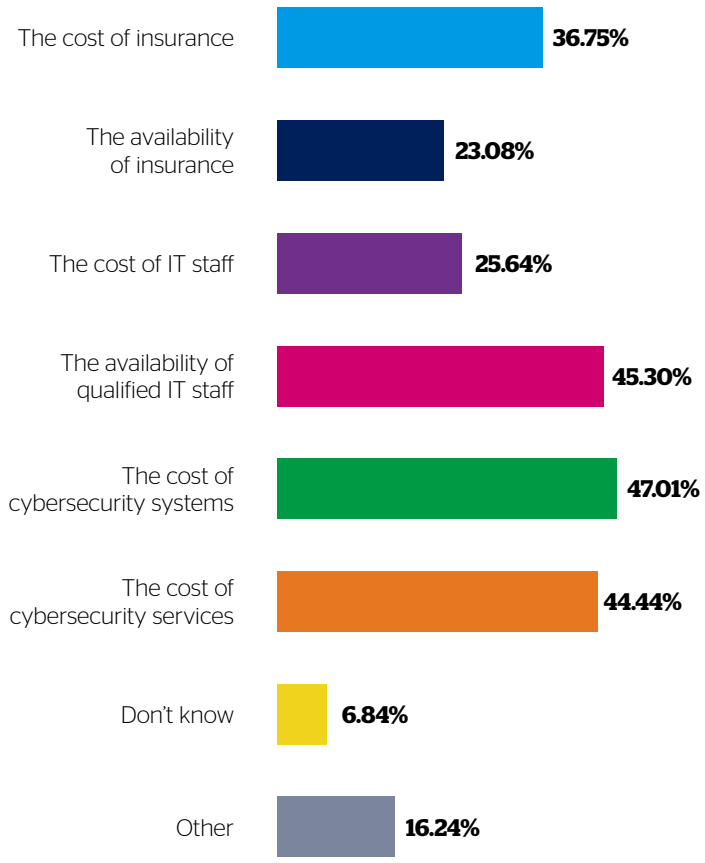
Beyond the actual risk transfer, respondents view carrier breach response services and incident response planning as the most valuable features of their cyber insurance policy. Although the overall perception of cyber insurance among the respondents has improved, many risk professionals overlook the other value-added coverages and services provided.

Depending on the carrier and the cyber insurance policy, the coverage features may include reimbursements involving network extortion, consequential reputational losses, business interruption, dependent business interruption and criminal reward funds, among others. Value-added services run the gamut, from threat intelligence, security assessments and network scanning resources to workshops and cyber data and information insights. Access to relevant vendors and advice on these services comes part and parcel with many cyber insurance policies.

The survey suggests these varied features could be better communicated by insurers and brokers: Nearly half (49%) of the respondents said a reason to interact with their cyber insurance carrier is to seek their advice on cybersecurity measures and risk mitigation strategies.

The survey findings suggest a variety of reasons why many respondents decided not to take advantage of the value-added services and coverages offered by brokers and insurers, in some cases for free. Organizations that have not filed a claim on their cyber

What, if any, of the following present a challenge for your business in managing cyber risk?



insurance policy may be unaware of the benefit of these ancillary policy features. Other respondents said they designed and drafted their own cybersecurity programs in advance of qualifying for insurance, rather than collaborating with carriers in these determinations and actions. Some survey respondents dismissed the non-risk transfer options outright, either viewing them as unnecessary or irrelevant.

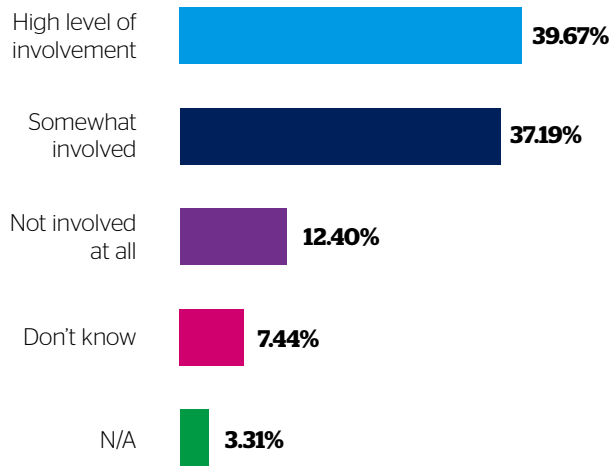
Insurers and brokers may benefit by demonstrating the value of cyber insurance beyond the opportunity for risk transfer, educating clients on the ancillary proactive and preventative risk management options that are also available.

The survey findings provide an opening for insurers and brokers to further demonstrate the value of cyber insurance beyond just the opportunity to transfer the risks. The findings allow for client education on the proactive and preventative risk management options that are also available in the policy.

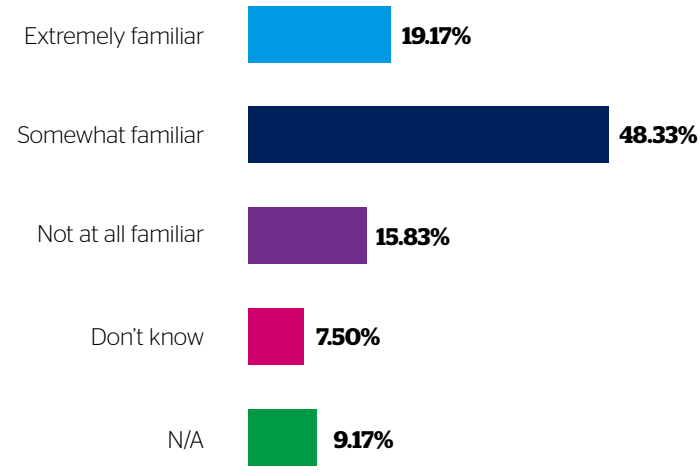
For example, non-risk transfer services like cyber data and information insights were valued by only 37% of respondents, suggesting these features could be better communicated by industry professionals.

Reaching out to directors and officers

How involved is your board of directors in your organization's cybersecurity?



How familiar is your board with your cyber insurance policy and related services?



The survey findings suggest that cyber insurers and brokers should seek to engage members of the C-suite in discussions on cyber risk transfer and related risk management and mitigation. While company risk managers are primarily responsible for cyber insurance purchasing decisions, CXOs and boards play significant roles in cybersecurity. They must ensure the entire organization understands the critical nature of cyber risks, is prepared well in advance of a potential breach and has the available resources to recover quickly from a potential business disruption.

Many respondents cited the cost of cybersecurity systems, services, and the availability of qualified IT staff as their top challenges in managing cyber risk, creating the opportunity for insurers and brokers to promote the value-added risk management coverages and services to chief information security officers. Asked how often their company's information security and risk management professionals discuss cyber insurance, only 38% of respondents said frequently, with 27% commenting "just around renewal time."

Although boards are either highly or somewhat involved in the organization's cybersecurity, directors may not be fully aware of insurers' proactive and preventative risk management options.

A similar opportunity exists to communicate the non-risk transfer services to board members more effectively. The survey findings suggest that board members may not be fully aware of the proactive and preventative risk management options provided in the cyber insurance policy. Nearly 50% of respondents said their boards are "somewhat familiar" with the cyber insurance policy and services, less than 20% are "extremely familiar" with the policy and services, and 16% are "not at all familiar." Given the different levels of familiarity, insurers and brokers can articulate the value of the policy's risk management features.

Vetting vendors

While the survey respondents view breach response services and incident response planning as valuable aspects of their cyber coverage, almost half (45%) did not rely on their insurers to develop these connections, reporting preexisting relationships with breach response vendors. Fewer than one-quarter (23%) of the respondents built these relationships with the help of their insurance partners, while slightly over 30% did not know if they had such relationships or built them.

Many survey respondents said they added their third-party vendors to the cyber insurer's preapproved panel. Others commented that their external vendor partners were not approved by their carriers (receiving insurer approval for external vendors is a complex decision factoring in the vendor's expense and experience).

As insurers and brokers engage in discussions with clients about potential claims scenarios and related remediation and recovery, they should cite the importance of the breach response services insurers provide to enhance cyber resilience.

Insurers and brokers who engage in discussions with clients about potential claims scenarios have an opportunity to illustrate the holistic value of the cyber insurance policy's breach response and incident response services. The discussion can expand to comprise the availability of other coverages and services offered in the policy to enhance the buyer's cyber resilience.

If organizations opt to rely instead on external vendors, insurers and brokers should, at the very least, emphasize the importance of having the cyber insurer approve their choices. Insurer-endorsed client vendor panels offer advance notice in the event of a claim, generating greater flexibility to assist the insured's specific needs. Absent insurer approval, friction could occur during the claims process.

Conclusion

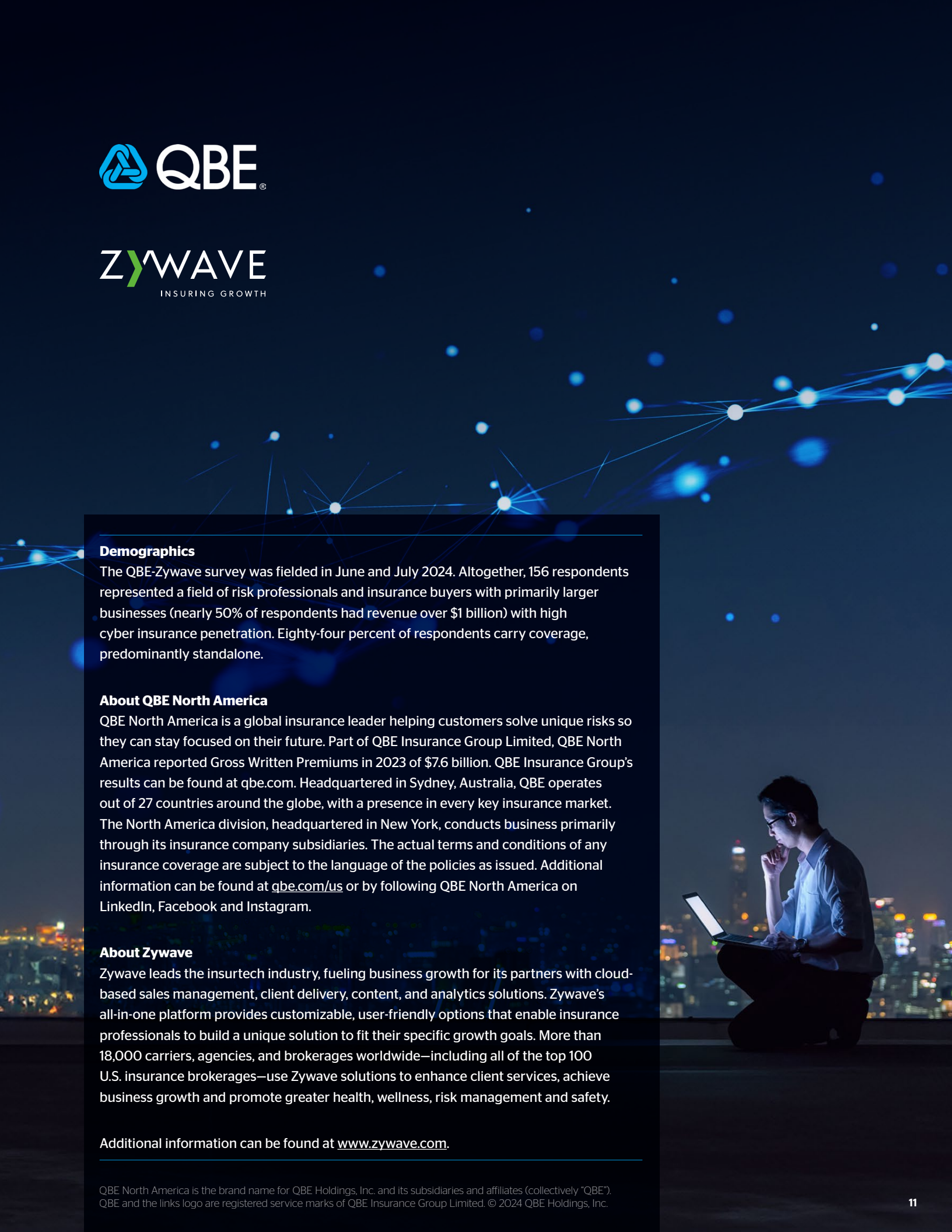
The survey illuminates several opportunities for insurers and brokers to increase the frequency and content of their communications with cyber risk professionals. Many respondents expressed interest in wanting more education about cyber threats, risk quantification and anonymized claims information, helping them to better understand the potential impacts. One respondent, for example, commented positively on the carrier's free educational videos and private educational sessions.

Although clients strongly perceive the risk transfer value provided by cyber insurance, the survey underscores the need for cyber insurance professionals to increase the frequency and content of their communications.

Regarding added value from an insurer beyond risk transfer, the survey responses indicate that increased awareness of risk management services is required. By clearly illustrating and emphasizing the value of these services and streamlining their access, insurers and brokers can enhance their client's cyber risk resilience.

As insurers and brokers engage in more frequent interactions with insureds, especially regarding the availability of additional cyber risk management coverages and services, a more positive opinion of the industry and its multifaceted benefits beyond risk transfer should result. By partnering together to manage, mitigate and minimize the business impact of cyber risks, clients will learn more about their risks, ensuring greater risk resiliency.

Check the top three reasons you want to interact with your cyber insurance carrier.



Demographics

The QBE-Zywave survey was fielded in June and July 2024. Altogether, 156 respondents represented a field of risk professionals and insurance buyers with primarily larger businesses (nearly 50% of respondents had revenue over $1 billion) with high cyber insurance penetration. Eighty-four percent of respondents carry coverage, predominantly standalone.

About QBE North America

QBE North America is a global insurance leader helping customers solve unique risks so they can stay focused on their future. Part of QBE Insurance Group Limited, QBE North America reported Gross Written Premiums in 2023 of $7.6 billion. QBE Insurance Group's results can be found at qbe.com. Headquartered in Sydney, Australia, QBE operates out of 27 countries around the globe, with a presence in every key insurance market. The North America division, headquartered in New York, conducts business primarily through its insurance company subsidiaries. The actual terms and conditions of any insurance coverage are subject to the language of the policies as issued. Additional information can be found at qbe.com/us or by following QBE North America on LinkedIn, Facebook and Instagram.

About Zywave

Zywave leads the insurtech industry, fueling business growth for its partners with cloud-based sales management, client delivery, content, and analytics solutions. Zywave's all-in-one platform provides customizable, user-friendly options that enable insurance professionals to build a unique solution to fit their specific growth goals. More than 18,000 carriers, agencies, and brokerages worldwide—including all of the top 100 U.S. insurance brokerages—use Zywave solutions to enhance client services, achieve business growth and promote greater health, wellness, risk management and safety.

Additional information can be found at www.zywave.com.