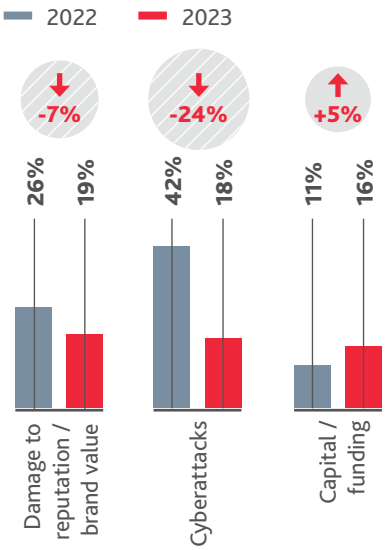
AMERICAS

BDO's Global Risk Landscape Report 2023 examines the 'risk multiplier' effect and how global businesses should be moving toward a more risk-welcoming approach.

Across the Americas, there is widespread acknowledgement of the risk multiplier effect, but are businesses making the paradigm shift to embrace a proactive approach to risk management? Encouragingly, the BDO Global Risk survey found that 81% of respondents in the Americas agreed the global risk landscape is better characterized by the relationships between risks rather than the risks themselves and 90% believe risks are becoming more interconnected and complex.

In terms of specific risks, the top threat that organizations across the Americas are unprepared for is damage to reputation and value, although at 19%, this is a drop of seven percentage points from the 2022 survey. Similarly, cyber attacks came in second at 18%, although this represents a significant drop from 42% a year ago. Likely the result of regional business leaders investing significantly in managing this risk over the last 12 months. Conversely, capital/funding risks took the third spot at 16%; this is an increase of five percentage points in the past 12 months, and is not surprising given the recent turmoil in the US banking sector.

FIGURE ONE: TOP THREE RISKS YOUR ORGANISATION IS UNPREPARED FOR



FOR MORE INFORMATION:

VICKY GREGORCYK

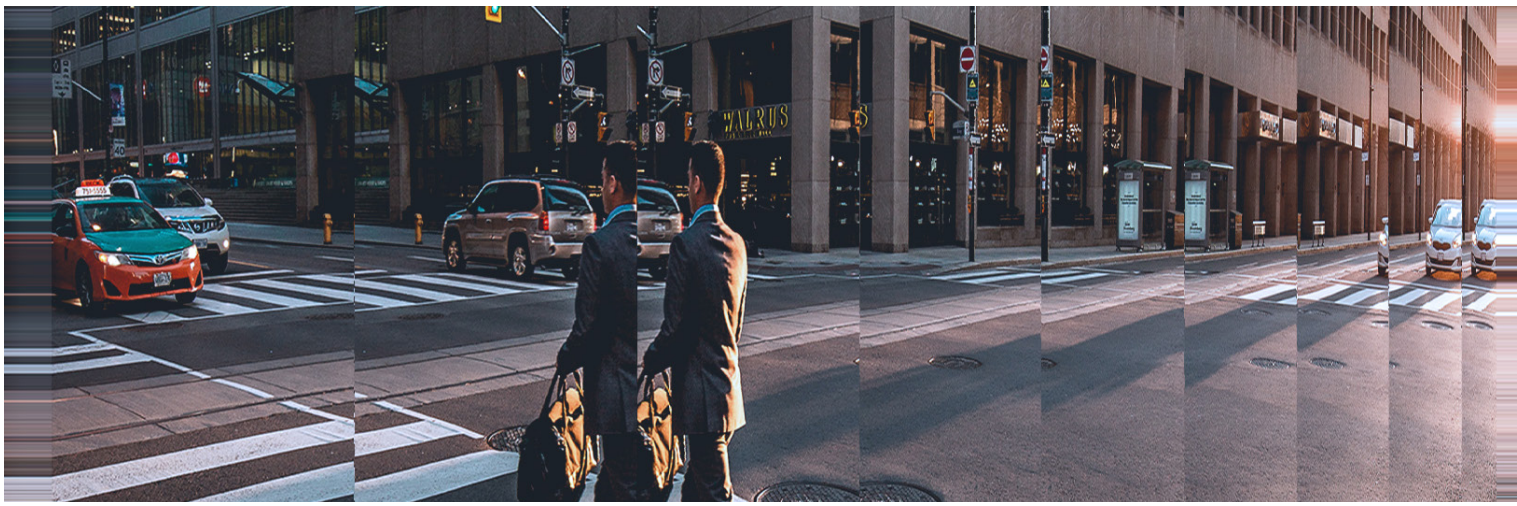
Managing Partner,
Risk Advisory Services,
BDO USA

vgregorcyk@bdo.com

ZIAD AKKAOUI

Partner,
Risk Advisory—Consulting,
BDO Canada

zakkaoui@bdo.ca



This year's survey recorded a 443% increase in respondents from the Americas saying their organization is "very proactive" in dealing with risk, shooting up from 7% in 2022 to 38% in 2023. On a practical level, this means businesses in the region are taking a range of steps to understand and manage risk multipliers. At 69%, the most common step taken is to implement early warning systems to detect and respond to risks spilling into other business areas, followed by conducting risk assessments to determine the multiplier effect (59%).

FIGURE TWO:

19%

said "damage to reputation / brand value" was the **No.1 risk** business leaders in the Americas felt their organisation was unprepared for

38%

said "cyber fraud and hacking" was the **No.1 fraud** risk Americas' respondents felt their business was most vulnerable to

FIGURE THREE: THE STEPS BUSINESSES IN THE AMERICAS ARE TAKING TO UNDERSTAND AND MANAGE RISK MULTIPLIERS

45%

Conduct audits to identify all potential risk multipliers

59%

Conduct risk assessments to assess risks and their multiplier effect

45%

Implement strategies designed to target the specific risk multipliers

69%

Implement early warning systems to detect and respond to risks spilling into other areas of the business

31%

Bring together expertise from across the organisation to help understand and manage risk multipliers and their impact

However, at the other end of the spectrum, only 31% of businesses in the Americas are bringing together expertise from across the organization to help understand and manage risk multipliers and their impact, which may affect how businesses deal with not just intersecting risk, but risk velocity as well.

Vicky Gregorcyk, National Managing Partner, Risk Advisory Services, BDO USA, says the pace of change within business is "much faster" than it has been previously: "There's going to be a risk to that [risk velocity], either on the upside, or potentially, the downside too, so companies always need to be talking about the risks involved and get the appropriate people from inside or outside the company involved to address the risk.

THE NEW TRADE-OFF IN CYBER RISK

Cyber risk is not only viewed as the top risk by organizations in the Americas, but it is a significant risk multiplier, spilling over into other business areas. This exposes businesses to increasingly sophisticated types of fraud, serious data security breaches, financial loss and brand reputation risks.

Ziad Akkaoui, National Practice Leader, Risk Advisory Services, BDO Canada, says there are similarities between the cyber risks faced by businesses in the US and Canada, particularly in terms of the evolution of the regulatory landscape: "The surge in cyber breaches has raised concerns about cybersecurity and privacy-related risks and vulnerabilities for information systems, highlighting the urgent need for enhanced cybersecurity measures. Similar to the US, the Canadian regulatory landscape is evolving to enforce mandatory disclosure of these breaches, ensuring transparency and accountability in the face of evolving cyber threats."

However, alongside the multiplier effect of cyber risks, a new trade-off has emerged with enormous benefits for businesses. Ever-advancing AI tools, such as ChatGPT and midjourney, come with risks such as third-party fraud, privacy and data security concerns, but this technology allows businesses to generate efficiencies, better communicate with customers, and enhance cyber protections.

Gregorcyk describes technologies such as AI as a "massive opportunity," citing its potential for internal audit processes as an example of how it can generate efficiencies with processing and interpreting large datasets: "Now, we can get the data. We do still use our thinking skills to look at the exceptions [that AI has identified], which adds more benefits to the company. We currently help a lot of companies build their data analytics programs into their overall internal audit methodology."

Among businesses in the Americas, the challenge of managing cyber risks is significant with 92% of respondents from the region saying their organization is struggling to handle the speed and sophistication of cyber attacks, and 82% naming cyber as the top risk priority for their organization. Despite the enormity of these challenges, 85% of respondents in the Americas are optimistic about AI technology, while only 11% are pessimistic.

FIGURE FOUR:

92%

of respondents in the Americas said their organisation was struggling to handle the speed and sophistication of cyber attacks

82%

said cyber risk was now the top risk priority for their organisation

85%

of respondents were optimists on AI in the Americas compared with only 11% who were pessimists

Gregorcyk attributes the attitude toward cyber risks in the Americas to awareness and ESG concerns, which intersect with reputational risks.

"Many companies are getting very sophisticated about [cyber risks] because you can see how much you're being attacked every day and how many bad actors you're keeping out," she says.

With the survey revealing that damage to reputation and brand value was the number one overall risk that business leaders in the Americas feel unprepared for, and cyber fraud and hacking was the top fraud risk, the magnitude of the multiplier effect is clear—technologies, such as AI, mean that as cyber criminals become more sophisticated, businesses will need to develop increasingly advanced tools to manage these intersecting risks to protect businesses.

Data protection in particular is a major concern with intersecting cyber risks, according to Akkaoui.

"Data governance is becoming more prevalent—there is so much outsourcing going on post-pandemic that it has led to dependencies on service providers and key vendors," he explains. "So, data governance is becoming more and more important as it provides a structured framework for organizations to manage, protect, and leverage their data assets effectively."

Akkaoui cites the example of Indigo Books & Music, Canada's largest bookselling chain, as an example of how a cyber attack is a risk multiplier. In February 2023, the company suffered a ransomware attack, which took the website offline and prevented online sales and in-store card payments. While no customer data was released to the public and the website went back online without a ransom being paid, the damage was significant. Financial and reputational losses were suffered as a result of the store being offline for a number of days—the company revealed that the attack cost them "millions of dollars" in lost revenue and expenses, and said it is improving cyber security measures in a bid to win back customer trust.

"AI tools are only going to get smarter and eventually could be utilized by malicious actors to develop more sophisticated hacking techniques, including ransomware" he cautions. "I don't want to be a pessimist, but I think these systems are going to get smarter and they're going to start building their own attacks if not regulated—it's a perfect storm."

Looking ahead, Gregorcyk and Akkaoui urge businesses to take a proactive approach to addressing cyber risk—and not just from a regulatory compliance approach. This allows management to focus on all of the impacts of cyber risks that can easily multiply and amplify other risks, including reputational and legal risks. They agree that businesses in the US and Canada can be very compliance-oriented. As such, leaders may not be considering the complexities of cyber risks, and better communication may be required to improve understanding of risk multipliers that can come from inside and outside organizations.