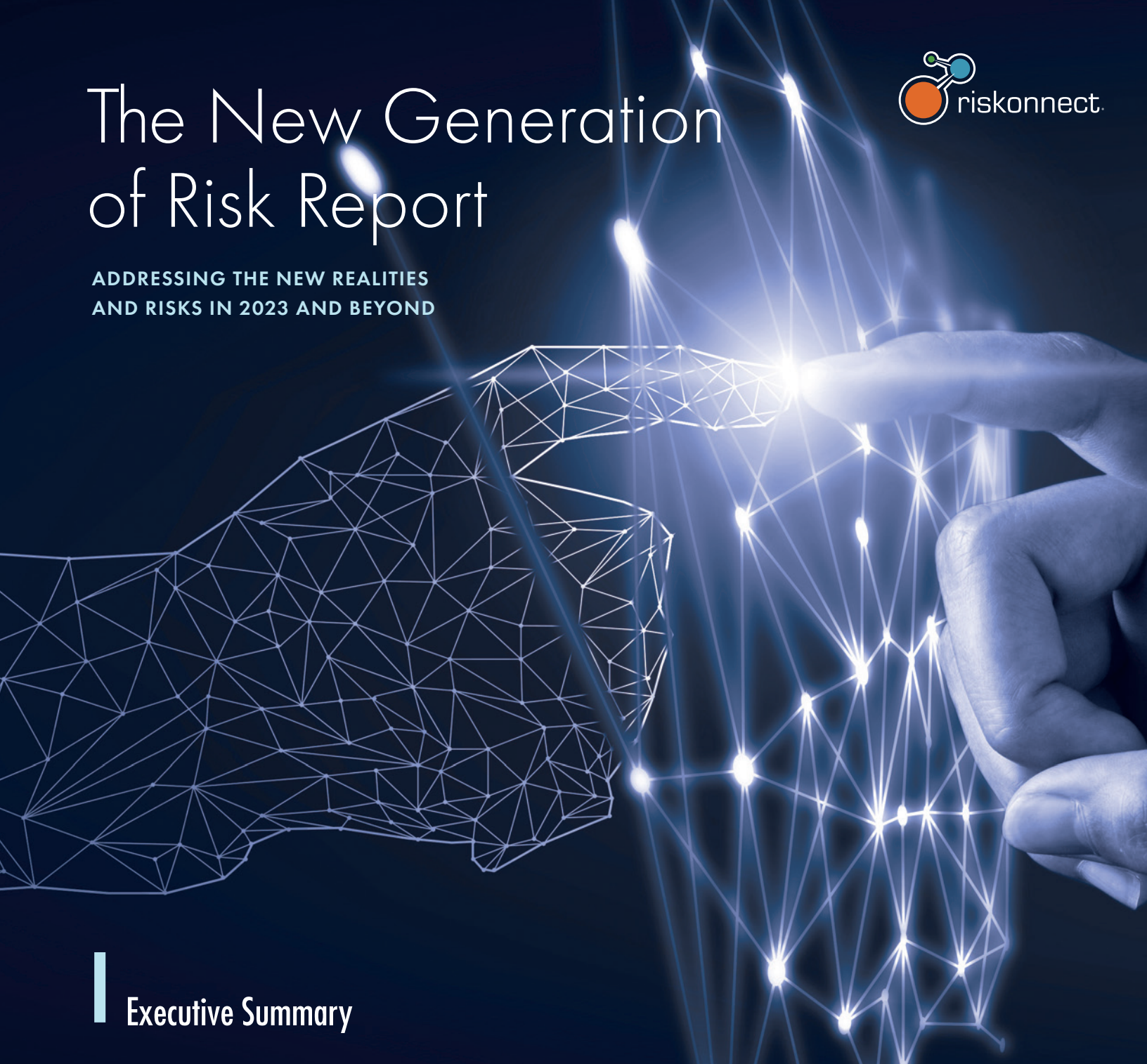
The New Generation of Risk Report

ADDRESSING THE NEW REALITIES AND RISKS IN 2023 AND BEYOND



Executive Summary

Generative AI tools like ChatGPT are changing how people work and raising unforeseen business risks. The current economic climate is creating new concerns. Ransomware, deepfakes, and other sophisticated cybersecurity issues are emerging and evolving at full speed.

Are organizations' risk management strategies evolving fast enough to keep up with this new generation of risk?

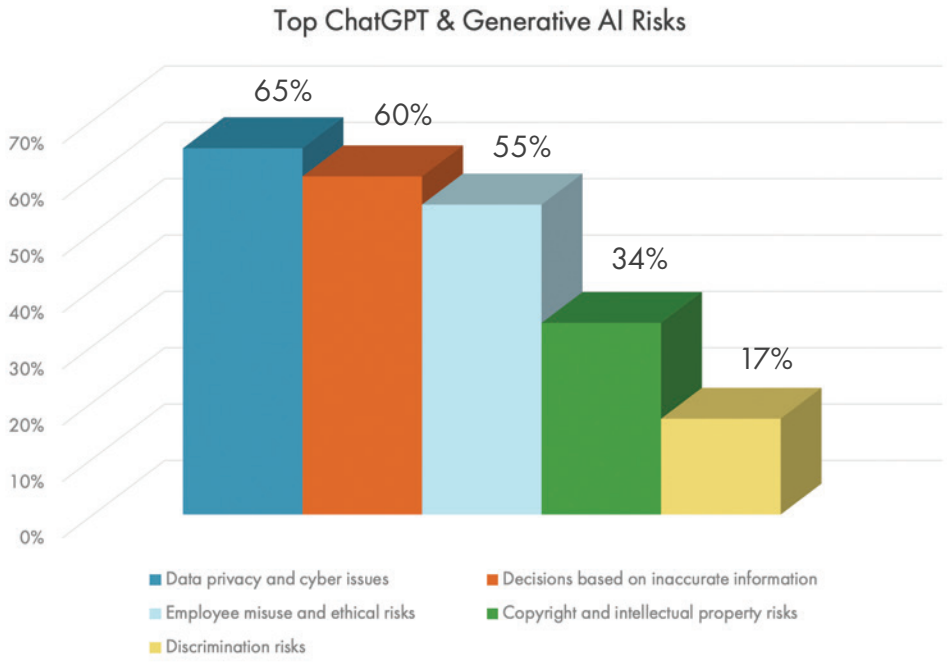
To find out, Riskonnect surveyed more than 300 risk and compliance professionals worldwide about the new threats facing organizations today and how they are revamping their risk management playbooks to navigate uncharted territory.

Riskonnect's 2023 **New Generation of Risk Survey** revealed that this convergence of new risks is increasing the pressure on companies to meaningfully change how they manage threats. Budgets are shifting. Risk management functions are growing. And strategies are changing.

The Rise of ChatGPT and Generative AI

Generative AI burst onto the scene, bringing a new wave of business risks. Most companies (93%) anticipate significant threats associated with generative AI, signaling a universal awareness of the transformative, yet potentially perilous, nature of this technology.

Companies' top concerns about AI include data privacy and cyber issues (65%), employee decisions based on erroneous information (60%), and employee misuse and ethical risks (55%). Copyright and intellectual property risks (34%) and discrimination risks (17%) were not far behind.



Just 9% of companies say they're prepared to manage generative AI risks, indicating a significant readiness gap.

Surprisingly, only 17% of organizations have formally trained or briefed their entire company on generative AI risks. The lack of urgency likely indicates the technology is moving so fast that companies don't know where to start. It could also mean companies aren't yet feeling the impact of these risks, but as generative AI gains adoption, that could quickly change. Generative AI is expected to reach 77.8 million users in the next year[1]. That's more than double the adoption rate of both tablets and smartphones.

According to the Riskonnect report, organizations have generally taken a "wait-and-see" approach when it comes to getting a handle on generative AI risks and implementing safeguards. But given the technology's high adoption rate, that mindset will need to shift – and soon. Especially as labor challenges persist and employees juggle multiple responsibilities, the appeal of technologies like ChatGPT as efficiency enhancers increases. Generative AI has the potential to automate work activities that absorb 60-70% of employees' time today[2].

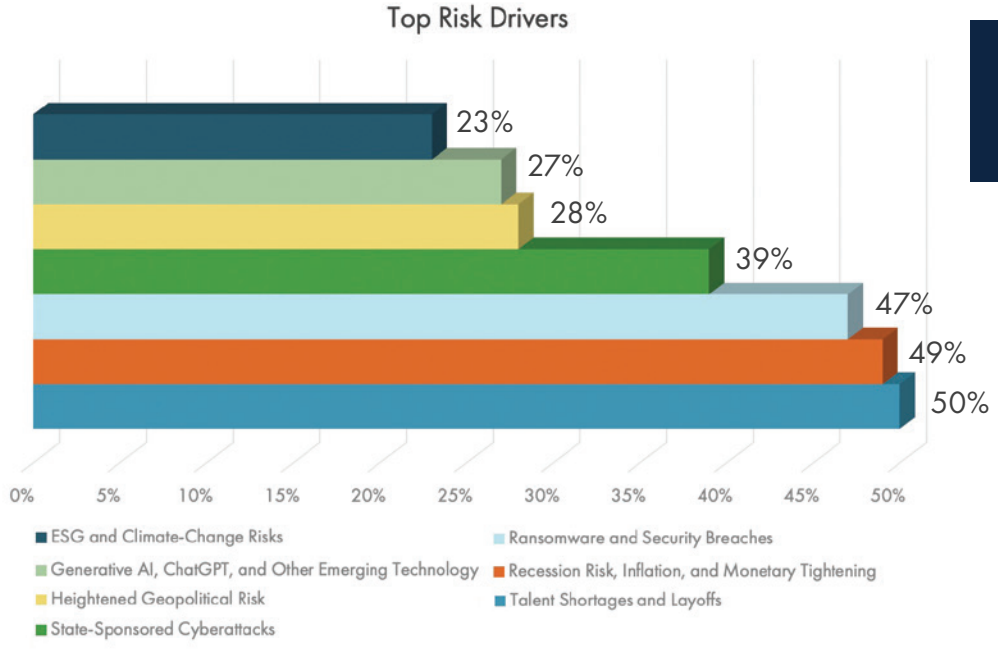
Getting a handle on the risks of generative AI now is paramount to successfully embracing and using the emerging technology as a value driver instead of fearing it as a source of risk.

---

[1]Insider Intelligence, "Generative AI adoption climbed faster than smartphones, tablets"
[2]McKinsey, "The economic potential of generative AI: The next productivity frontier"
[3]Security Magazine, "68% of organizations face cyber risks due to skills shortage"
[4]Semiconductor Industry Association, "America Faces Significant Shortage of Tech Workers in Semiconductor Industry and Throughout U.S. Economy"
[5]Wired, "Ransomware Attacks Are on the Rise, Again"
[6]IBM, "Cost of a Data Breach Report 2022"
[7]Fintech Nexus News, "How AI is fueling the fraud surge: Sift report"

The Economy and Worsening Skills Shortages

Today's market conditions continue to create significant risks for companies. Organizations cite their top risk drivers overall as talent shortages and layoffs (50%) and the economic environment (49%).



Risks companies say are having a severe or significant impact on their organizations

Many companies can't find and hold onto the skilled workers they need, which raises considerable risks and threatens the global economy. Sixty-eight percent of organizations face a higher risk of cybersecurity issues because of the skills shortage[3]. Major industries – tech, finance, airlines, food service, retail, and more – are strained by talent shortages. The semiconductor industry, which props up the economy, has 1.4 million technician, computer scientist, and engineering jobs at risk of going unfilled by 2030[4].

A Spike in Cybersecurity Events

Ransomware and security breaches (47%) came in third for risks with the biggest business impact. This isn't surprising given that 2023 is on pace to be one of the most expensive years yet in terms of ransomware payments, forecasted at $898.6 million[5]. The average cost of a ransomware attack – not including the cost of the ransom itself – is $4.45 million[6]. The likelihood of being a target of such an attack could increase even faster with the adoption of generative AI, which enables hackers to create more personalized and realistic phishing emails to infiltrate and take control of companies' systems. In fact, AI is behind a more than fourfold increase in account hacking attempts in the first quarter of 2023 compared to all of 2022[7].

Interestingly, out of the top risk drivers, 45% of director and C-level risk leaders feel very prepared to tackle ransomware and security breaches, while only 17% of director and C-level risk leaders feel very prepared for talent shortages.

Thirty-nine percent of risk and compliance professionals say state-sponsored cyberattacks have a significant or severe impact on their business. When asked about which regions companies are most concerned about when it comes to geopolitical risks, Eastern Europe (Russia and Ukraine; 32%) and East Asia (China and North Korea; 22%) topped the list.

C-suite executives may feel more prepared for ransomware given that while security breaches can have a material impact on the organization, companies can invest in cyber insurance and technologies to fight these issues. The roadmap for tackling talent shortages is less clear. The challenges run deep and require a multipronged approach of upskilling, employee engagement programs, contractors, automation, and more to close the gap.

> **Companies often turn first to insurance to help reduce the impact of cybersecurity issues, but getting cyber insurance is not always a simple task. A business continuity plan with emergency notification capabilities can speed response, which will reduce the likelihood of experiencing significant downtime.**

Evolving Regulations

When asked about the specific regulations that keep teams up at night, data privacy regulations, including General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and the Personal Information Protection Act (PIPA), were a top concern (40%). Almost equally pressing are regulations tied to ESG considerations, including new reporting rules and supply chain and due diligence laws (32%), followed by financial regulations at 9%, specifically anti-money laundering, financial crimes, and SOX compliance.

Employee Burnout and Strategic Risks

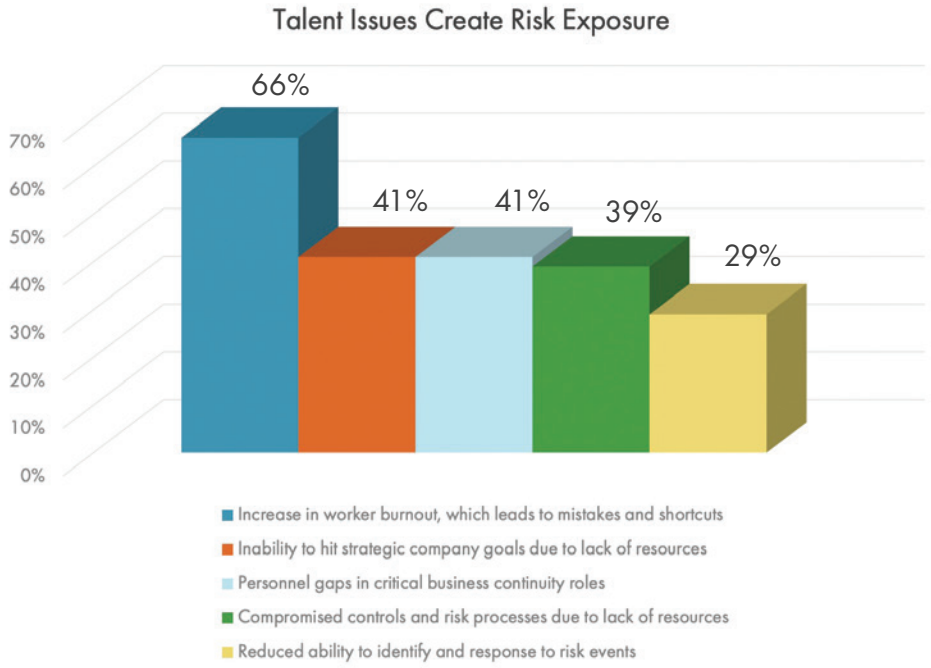
A whopping 85% of companies said they have been affected by labor shortages. Half of companies report significant or severe business impacts resulting from talent issues.

Talent shortages and layoffs profoundly increase organizations' risk exposure and affect businesses' ability to perform. The biggest risks companies associate with labor shortages and layoffs are:

- Mistakes and shortcuts driven by worker burnout (66%)
- An inability to reach strategic goals (41%).

When organizations operate with fewer staff, existing employees often pick up the slack, which increases the likelihood of burnout and errors — and takes their time away from the most important initiatives.

Companies that are slow to address talent shortages increase their risk exposure and threaten their organizational resilience. Personnel gaps in critical business roles (41%) was cited as the third biggest issue stemming from the talent shortage, indicating companies could face severe business interruptions if a crisis hits.



Companies Force Change

Finally, companies are changing how they govern, prioritize, and oversee risk.

Companies' playbooks for managing the "new generation of risk" are evolving almost just as fast as the threats they face.

The most noteworthy shift is the emergence of chief risk officers (CROs). Over half (52%) of organizations now have a CRO. Another 6% plan to hire one in the next 6-12 months. This is a dramatic improvement from just three years ago where one study indicated only 20% had a CRO at the helm[9]. Following several years of chaos and disruption, more organizations are realizing the value of centralized, C-level risk oversight in managing all facets of risk. They're also realizing the criticality and value of risk managers in protecting the organization.

Eighty-two percent of respondents said their risk management team headcount has increased or remained the same in the past six months. This expansion, especially against a backdrop of layoffs, talent shortages, and uncertain economic factors, highlights the crucial role these professionals play in guiding organizations through the complexities of this new risk landscape.

> Data is the lifeblood of risk management teams. The strength of a company's risk intelligence and reporting capabilities determine how effectively it can identify, manage, and respond to risks.

Over 38% of people today are burned out[8] – a figure that has been trending upwards over the past few years. Employee burnout impacts the bottom line through lower productivity, worker absenteeism, higher employee turnover, medical costs, safety issues, mistakes, and more.

Automation can be a lifeline for companies suffering from talent shortages. Streamlining core tasks can help existing talent get their work done faster, alleviate stress and burnout, and reduce the likelihood of mistakes and errors. Automation also frees talent up to focus on strategic priorities so the organization can meet its goals.

Alongside the growth in risk management teams, spending on risk management technology has held steady, despite the economy. Nearly a third of companies (28%) reported budget increases for risk management technology in the past six months. This affirms the value technology plays in helping risk managers protect their organizations. As companies invest in technology and automation to support their risk functions, risk managers can get more done and focus their time on mitigating and managing the risks that are most harmful to the organization.

Companies looking to invest in risk management technology would be best served by prioritizing tools with strong data quality and reporting capabilities. Only 23% of respondents say they're very confident in the accuracy, quality, and actionability of their risk management data. Just 5% are very confident in their ability to extract, aggregate, and report on risk insights to fuel decisions.

> *"If no action is coming out of the data, what's the point?"*
>
> Trey Braden
> *Director of Risk Management*, Randstad

On the positive side, 70% of organizations say they have adequate collaboration across the different lines of defense for financial risk and 69% say the same for operational risk.

[8]Shift the Work, "Top 5 Things You Don't Know About Burnout in 2023"
[9]Insurance Business, "Only one in five UK firms has a chief risk officer, finds Gallagher"

Scenario Planning: Closing the Gap

While companies are finally changing how they govern, prioritize, and oversee risk, the majority of companies (63%) have not simulated their worst-case scenarios, which most respondents said revolve around natural disasters, cyber, and geopolitical risks.

This finding is surprising considering the "worst case" scenarios and risk events of the past few years. The COVID-19 pandemic. The series of severe global supply chain disruptions that followed. Most recently, the Silicon Valley Bank collapse and subsequent bank failures. Organizations have been hit with or witnessed many disruptive events that at their core were known and predictable and yet robust scenario planning is still not a priority for most.

Has your organization simulated its worst-case scenario? Now is the time.

The Silicon Valley Bank collapse was a near worst-case scenario for many businesses. Despite the scale and global economic impact of the collapse, nearly (42%) of those that said the collapse was relevant to them have not made changes to their risk management strategy as a result. Scenario planning is a key part of risk management and needs to be incorporated into strategies going forward to build resilience.

Only 5% of organizations feel prepared to assess, manage, and recover from a future unknown and unpredictable risk event.

> *"Risk management is about managing uncertainty. When the business becomes uncertain, that's where the ability to sit in the control tower, understand what's approaching, have visibility on what might happen next – including the peripheral effects – and how that could impact the business is what gives you a firm risk-visible foundation to define response strategies. Then you can use these strategies to adapt and pivot according to the way a particular situation plays out."*
>
> Bob Bowman,
> *Sr. Director, Chief Risk Officer*
> *Risk Management, Enterprise Data Governance*
> The Wendy's Company

Preparing for Risk Events: Companies Could Be Doing More

Another notable and positive shift: three out of every four companies (73%) are updating their business continuity plans to prepare for crises. But are these plans specific, tested, and comprehensive enough to help companies minimize the impact when something goes wrong?

Most companies today rely on piecemeal business continuity plans that are either built-in silos or fail to consider the cascading nature of risk. The problem with these approaches is that issues that seem unrelated or isolated to a specific department can spread to create bigger disruptions and bring the business to a screeching halt. Unless everyone across the organization is working from the same playbook, business continuity plans are created in vain.

The other common gap with business continuity planning is a lack of alignment between stakeholders on risk tolerance. Say an organization is planning for a potential ransomware attack. Executives think the organization can get the network back up and running within a few days. In reality, however, IT needs weeks. The problem: the stakeholders never conferred.

This lack of alignment among key stakeholders is all too common. One of the ways organizations can overcome this challenge is by facilitating risk workshops. These workshops get all relevant stakeholders in the same room to have real and productive conversations about the organization's preparedness, tolerance, and plan for specific risk events. Using the ransomware example, important points to talk through include:

- What would happen if the business were hit with a ransomware attack today?
- How much downtime it can tolerate?
- How long would it take to get back up and running?
- Would we consider paying the ransom – and what are the implications of both answers?
- How would you communicate to customers, partners, employees, and investors?
- What other risk events could cascade from this event and hurt the organization?

Thirty-seven percent of organizations are conducting risk workshops today, which is encouraging. Other measures companies are taking to prepare for crises include:

- Continuously re-evaluating their risk environment (66%)
- Assessing crisis response plans (64%)
- Preparing leadership to manage unexpected crises (53%)
- Collaborating with cross-departmental stakeholders (51%)

Expand Your Playbook

Many of the threats companies face today, such as generative AI, are just starting to take shape. There are still many unknowns in this new generation of risk, but one thing is certain: Companies need a new way to manage risk and defend their organizations:

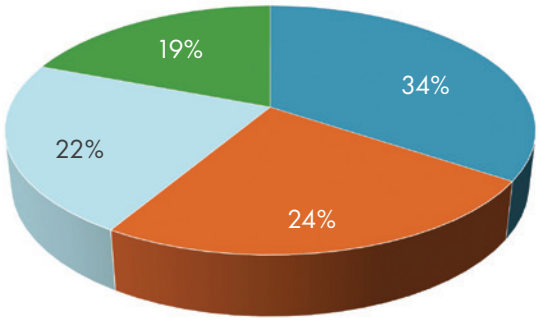
- Get all stakeholders and executive leaders on the same page about risk.
- Start planning for your worst-case scenarios.
- Invest in technology that helps combat the full spectrum of risk.
- Create true visibility into your risk exposure inside and outside of your organization.

If you add these four things to your playbook, you'll be better positioned to respond to threats, make decisions, limit disruptions, and maximize opportunities in this new generation of risk.

About Riskonnect

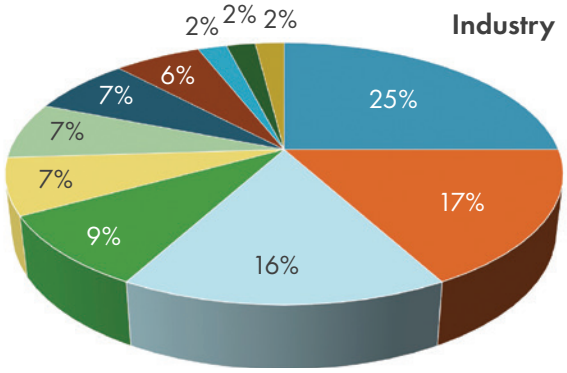
Riskonnect is the leading integrated risk management software solution provider. Our technology empowers organizations with the ability to anticipate, manage, and respond in real-time to strategic and operational risks across the extended enterprise. More than 2,000 customers across six continents use our unique risk-correlation technology to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 800 risk management experts in the Americas, Europe, and Asia. To learn more, visit www.riskonnect.com.

Role



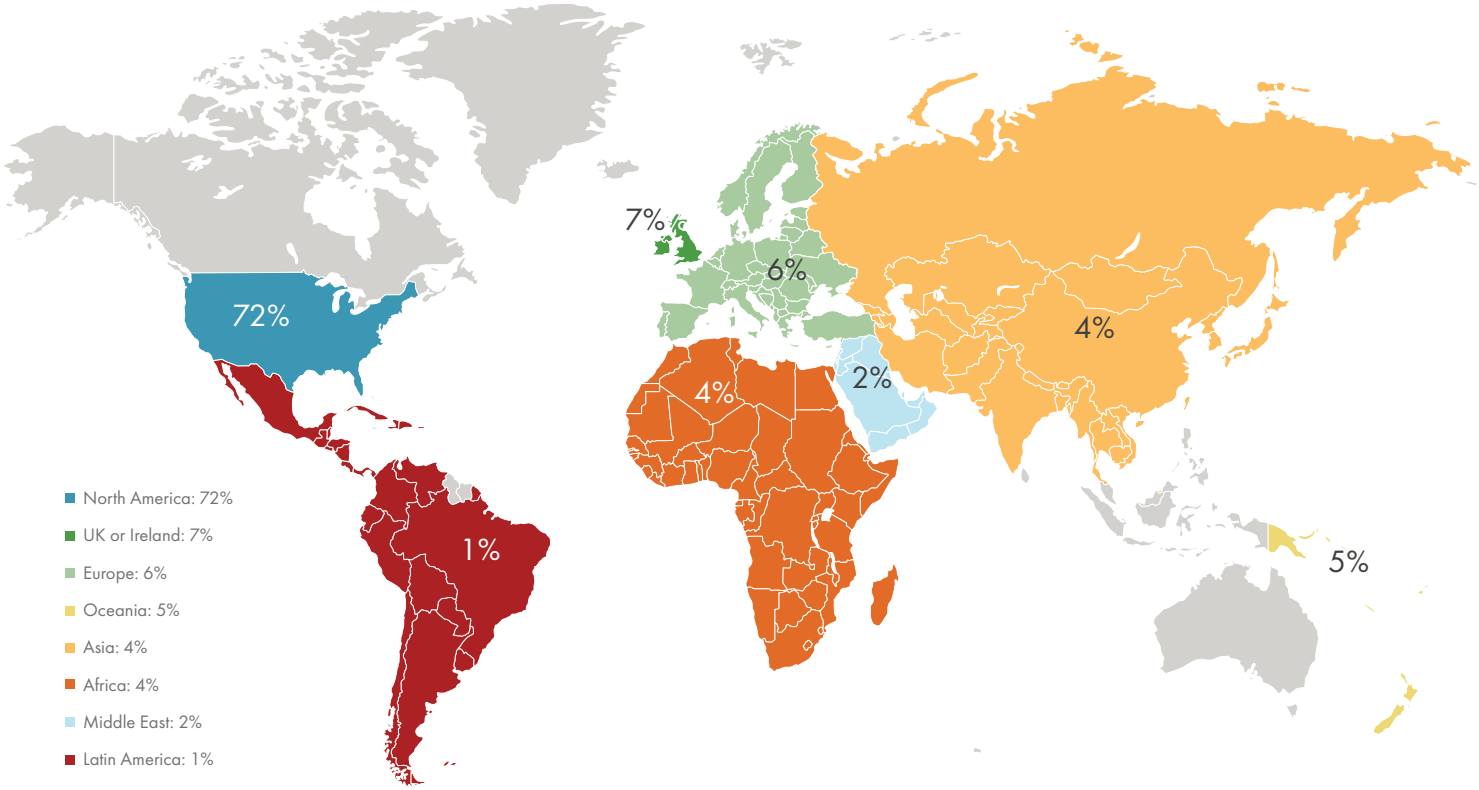
- Director in risk or compliance
- Analyst, specialist, or coordinator in risk or compliance
- Manager in risk or compliance
- VP or C-level risk or compliance executive

Industry



- Financial Services
- Public Sector
- Healthcare
- Infastructure
- Retail
- Manufacturing
- Insurer and TPAs
- Energy
- Transportation
- Insurance Brokers
- Aerospace and Defense

Geographic Location



- North America: 72%
- UK or Ireland: 7%
- Europe: 6%
- Oceania: 5%
- Asia: 4%
- Africa: 4%
- Middle East: 2%
- Latin America: 1%

A total of 303 risk and compliance professionals responded to the survey.