IRON MOUNTAIN®

White paper

The digital side of risk

Research and recommendations from the 2023 Economist Impact Risk Reset study

Summary

Recently, Economist Impact conducted a global study sponsored by Iron Mountain that investigated how risk management is changing. The resulting paper examines that study's data from a technological perspective. It considers how digital transformation both contributes to and helps to mitigate risk. It highlights some of the most important findings from the survey and offers recommendations for improving risk management as it relates to digital technologies.

Contents

Risk reset

Over the last three years, organizations have learned a lot of firsthand lessons about business risk. They've survived a worldwide pandemic that altered the way we work. They've watched as international conflict led to further disruptions in the supply chain and skyrocketing fuel prices. They've weathered storms, fires, and other natural disasters that resulted in outages and financial losses. They've defended their digital systems from barrages of cyber attacks. And they've strategized ways to deal with worker shortages and rising inflation.

These experiences have changed the way organizations view risk.

To find out exactly how risk management is changing, Iron Mountain sponsored a global study conducted by Economist Impact. The firm conducted primary research to understand how executives perceive the key internal and external factors shaping an organization's approach to risk and the role that executives, technology, and the institutional setup play in risk management. Economist Impact surveyed 656 executives across key industries in Australia, Brazil, Canada, France, Germany, Hong Kong, India, Mexico, New Zealand, Singapore, the UK, and the US. They also consulted with risk management experts at The Clearing House, the World Economic Forum, and the Wharton School.

The resulting report, titled Risk reset: shifting focus from reaction to anticipation, delves deep into four key pillars of risk management:

1. Workplace evolution
2. Cyber security and data governance
3. Sustainability
4. Operational efficiency

In this paper, we'll take a closer look at the interplay between technology and these four pillars. We'll examine four key findings that shed light on how the digital landscape is affecting risk perception and management. And we'll look at four recommendations that arise out of the study's results.

4 key digital technology findings

The survey revealed that risk management has become a key focus for organizations over the last three years. In fact, 90% of executives said that identifying risks has become more important.

In addition, it found that technology plays a complex role in risk management. Here are four of the most important takeaways that relate to digital technology:

1. Digital risk and opportunity go hand in hand.

In the survey, 80% of executives said that technology offers their greatest risk, and their greatest opportunity. This dichotomy provides the foundation for understanding the relationship between digital technology and risk management.

In its analysis of the survey data, Economist Impact wrote, "Emerging digital technologies such as machine learning and artificial intelligence (AI) promise to expand the risk manager's toolkit, spotting patterns in data that human analysts might miss. However, attackers also have access to these technologies, which could be used to find vulnerabilities or launch more persuasive phishing attacks."

In many ways, the threat of cyber attacks is one of the most real and pervasive threats organizations face today.

The US Federal Bureau of Investigation received 800,944 cyber crime complaints in 2022 alone, with total reported losses of more than $10.3 billion. Most large enterprises repel cyber attacks on a daily basis, and those attacks are becoming increasingly sophisticated, particularly as nation-states become more involved.

And it isn't just their own systems that need protection. When companies use software and services from third-party vendors, they open themselves to additional risk. Simeon Fishman, executive vice president and CRO at The Clearing House, explained, "For example, only a few vendors provide cloud services, which has the potential of resulting in cloud concentration. A tech-centric organization, through the software they use or develop, may unwittingly put all their eggs in one or just a few baskets."

However, the solution isn't to avoid technology. On the contrary, failing to capitalize on emerging digital trends can actually expose companies to a different kind of technology risk — the risk of falling behind the competition.

In addition, technology can help companies to mitigate some kinds of risk. For example, backup and disaster recovery services, cloud storage, cyber security software, data analytics, and other tools can help organizations be better prepared for adverse events, potentially preventing downtime and data loss.

As they work to create their risk management strategy, organizations need to remember that digital technology is both a risk, and a mitigation tool.

2. Technology risk indicators are becoming more important.

Risk indicators are quantitative or qualitative signals that allow organizations to assess their risk level. The survey asked executives to indicate whether risk indicators from a variety of categories had become more or less important over the past three years. Across the board, an overwhelming majority of respondents said that each of the categories — reputational, operational, environmental, technology, and workforce — had become more important.

Reputational indicators, which include media coverage, customer complaints, and social media sentiment, showed the strongest change in importance, with 80% of executives saying this category had become more important. But technology indicators scored very high as well, with 76% saying this category is more important, 16% saying there was no change, and only 8% saying technology indicators were less important.

Technology risk indicators can include metrics that the IT teams probably already track, such as the number of cyber security incidents, network uptime, total software bugs, and mean time to resolution. They can also include more qualitative metrics measures that arise out of proactive risk management efforts. For example, you might measure the percentage of key roles in the organization for which you have a succession plan, or you might assess the effectiveness of your current IT risk management procedures.

The fact that executives are paying more attention to these indicators is a positive sign. It demonstrates that leaders are becoming more aware of how critical technology is to the business. It also reveals that digital transformation is having a widespread impact with the organization becoming more dependent on technology than ever.

3. Technology risk drives risk management improvement efforts.

The survey not only asked executives to look back at the last three years, but also to look ahead at where they want their risk management efforts to take them. In particular, it asked which kinds of risks would be driving their organizations' efforts to improve risk management over the next three years. The top vote-getter, with 43% of respondents, was technological risks. It even beat out financial risk, which was selected by 41%.

What kinds of technology risk are executives worried about? Examples include the following:

- **Cyber security:** Malware, ransomware, phishing attacks, denial of service, hacking attempts, and other types of cyber crime could expose sensitive information, result in downtime, and/or result in higher costs for the organization.
- **Downtime:** Hardware or software can experience issues that result in services being offline, sometimes for extended periods.
- **Third-party dependencies:** Products or services that you offer might rely on vendors who can experience outages, expose you to cyber attacks, or go out of business.

- **Obsolete technology:** If you rely on out-of-date technology, you may face operational challenges or expenses associated with upgrading.
- **Integration problems:** As you deploy new technology, you may face unforeseen issues with getting it to work with other systems and software.
- **Data loss:** Even if you don't experience a cyber attack, you can lose data due to theft, hardware or software failure, natural disasters, or other causes.
- **Regulatory changes:** Governments can pass new regulations that can impact the technology you use and develop.
- **AI risks:** The rapid rise of artificial intelligence has organizations concerned about potential issues related to bias and ethics.

Why are these risks driving improvement efforts more than others? The answer might relate back to the idea that technology risk and opportunity go hand in hand.

Organizations can address many of these technological risks by implementing new technology. And that new technology, in turn, offers opportunities to improve operations.

4. Data analytics and AI play a key role.

The study highlighted two key technologies that organizations are relying on for risk management improvements. Right now, interest in AI, particularly generative AI, is very high, so it might not be surprising that more than 8 out of 10 (83%) of executives said that they are using AI and cognitive technology in their risk management processes.

Similarly, 80% of participants said that their organizations are using data analytics in risk management "somewhat" or "significantly." That also seems to make sense given the high interest in analytics across all disciplines and industries.

Both AI and analytics help organizations find patterns in their data. And if they can see the circumstances when difficulties have arisen in the past, they might be better able to spot similar situations in the future.

How are organizations mitigating data and cybersecurity risks

The organizations in the Economist Impact study had already taken a number of steps to address digital risks. Here are some of the most common, along with the percentage of respondents that had implemented them:

Disaster recovery/business continuity plans for digital systems	92.2%	Guidelines for data collection, storage, and governance for remote workers	90.4%
Advanced technologies (e.g., AI/ML, cloud, IoT, quantum computing)	91.9%	Investment in asset lifecycle management for hardware and devices	90.1%
Cleanup of legacy physical and digital documents, files, and data	91.3%	Centralized technology function with full visibility into all info and tech systems	89.9%
Investment in IT and cybersecurity talent	90.9%	Changes to overall security infrastructure	89.8%
Revamped data compliance policies and IT standards	90.7%	Training on technical/data literacy	89.8%
Ongoing monitoring and prevention of cyber risk and threats	90.5%	Cloud services/storage	89.3%
Rethinking of chain of responsibility for managing IT and data governance challenges	90.4%	Hybrid work data protection and security applications	89.0%
Digitization of physical records for each of access/safekeeping	90.4%		

While AI, analytics, and other advanced digital technologies can be helpful, they aren't a complete solution in themselves. Fishman warned, "Technology can only get you so far if you don't have the right design, risk architecture, or data within your systems." He added, "It is also critical to understand how business processes and data are connected. Once the design and data are in place, analytics and data interrogation tools can be leveraged to form a more comprehensive understanding of risk in an organization."

That comprehensive understanding is really key — and one of the biggest areas where organizations have room for improvement when it comes to digital aspects of their risk management.

5 recommendations

The study also asked executives about the benefits and challenges of their current risk management activities. It asked them what was going well and where they wanted to improve.

Five key recommendations relating to digital technology emerged from that data:

1. Avoid an either/or mindset.

It's easy to fall into the trap of seeing risk mitigation and operational efficiency as mutually exclusive goals. In fact, in the survey, 65% of executives agreed that investing in long-term risk management impacts operations negatively in the short term.

In reality, organizations often report that they are able to both manage their risk and accomplish their business goals at the same time. More than that, many find that good risk management helps them achieve their other objectives.

In the survey, 41% of respondents said that their risk management had a "significant positive impact" on their operational efficiency. Similarly, 41% observed improved strategic decision-making and 42% reporting improvements in facilities and workspace planning.

Instead of viewing risk management as a tradeoff against innovation and efficiency, look for ways to use technology to improve your risk management that can also enhance innovation and efficiency. That can focus your efforts on areas that will provide the biggest benefit to the organization. For example, tools like workflow automation reduce risk by preventing human error, while also streamlining operations.

2. Look for ways to improve collaboration.

One of the strongest findings in the Economist Impact report is the need for organizations to improve their collaboration capabilities. The executives who participated in the study clearly understood that cross-functional collaboration is critical to risk management success. More than three-quarters of those surveyed (77%) agreed that risk management should consider all parts of the organization.

However, the respondents also acknowledged that they aren't doing as well in this area as they should be. More than half (57%) said that their organization needs to improve cross-functional collaboration. And 60% said they need to improve employee engagement and information sharing among functions, teams, and external partners.

In the report, Sophie Heading, global risks lead at the World Economic Forum, noted that collaboration can be particularly important when unforeseen outside events threaten the organization. "External factors exert a significant impact on organizations and necessitate cross-collaboration to address them," she said.

3. Make strategic investments.

While organizations are making some investments in talent and tooling that will help them improve their risk management capabilities, the report indicated that they likely should be doing more. A large majority (62%) of executives said that their organization needs to do better at proactively dedicating sufficient financial, technological, and human resources to risk management.

In particular, digital initiatives seem to be an area where respondents believe they need to put money. More than half (52%) of respondents plan to invest more over the next three years in risk management practices that more directly align with their dependence on digital. In addition, 59% said they needed to improve integration of new technologies or digital tools to promote better risk management practices.

The study also revealed that investment in two areas critical to risk management seems to have declined. Only 28% of survey respondents reported purchasing technology or digital tools to facilitate cross-functional data and information exchange since 2020. By comparison, 70% said the same before 2020. That is a concerning choice given that organizations want to encourage more cross-functional collaboration.

Similarly, only 29% have spent money since 2020 on cloud-based technology or digital tools to improve workflow automation and business processes. Again, the percentage was much higher — 69% — before 2020. Because automation can help reduce manual errors in process, this also seems like a number that is trending in the wrong direction.

4. Focus on resilience.

Risk management and resilience are closely related but slightly different.

Risk management requires organizations to identify possible risks and then take steps to reduce the risk. Resilience places the emphasis more on recovering quickly from adverse events, particularly when they are unanticipated. And while risk management pays a lot of attention to negatives — all the things that could go wrong, resilience turns attention to the positive — what you can do about challenges that arise.

Larry Jarvis, SVP and Chief Information Security Officer at Iron Mountain, explained that resilience helps organizations to not just survive but to thrive in the midst of difficult circumstances. "By building resilience against potential future threats rather than merely responding to familiar ones, organizations are capable of adapting to unforeseen risks and seizing emergent opportunities," he said.

Not matter how good your risk management capabilities are, your organization will eventually face hard times. By developing resilience alongside your risk management expertise, you put your organization in a good position to weather the storms that arise.

5. Seek out strong partners.

The turmoil of the past few years has made it more apparent than ever that our world is highly interconnected. Challenges in one industry or one part of the world ripple throughout the economy.

One important aspect of risk management is to seek out partners that have strong risk management capabilities themselves. In the digital world particularly, you need to know that your vendors, suppliers and partners are doing everything they can to avoid downtime or other events that could affect your business. With strong partners, your organization becomes stronger.

For more than 70 years, Iron Mountain has empowered customers worldwide to mitigate risks. It has helped thousands of organizations find ways to use technology to improve risk management and build resilience. See the Economist Impact study.

Learn more about risk management

Want to take a deeper dive into the insights uncovered by the Economist Insight Risk Reset study? Here are some additional resources:

Infographic	Risk reset: shifting focus from reaction to anticipation
Blog post	Risk amplified: cultivating risk awareness across the organization
Economist Impact white paper	Risk reset: shifting focus from reaction to anticipation
Article	Risk reset: anticipating what lies ahead
Website	Amplify risk management. Strengthen resilience. Empower your organization.

About Iron Mountain

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 225,000 organizations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of valued assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include information management, digital transformation, secure storage, secure destruction, as well as data centers, cloud services and art storage and logistics, Iron Mountain helps customers lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working.

IRON MOUNTAIN®

800.899.IRON | ironmountain.com