ECONOMIST IMPACT

Risk reset: shifting focus from reaction to anticipation

Sponsored by

IRON MOUNTAIN®

Contents

About the research and acknowledgements

Risk reset: shifting focus from reaction to anticipation is a research programme conducted by Economist Impact and sponsored by Iron Mountain examining key internal and external factors shaping an organisation's approach to risk and the role that executives, technology and the institutional set-up play in risk management. Economist Impact leveraged data from expert interviews and a bespoke survey of 656 executives across key industries in Australia, Brazil, Canada, France, Germany, Hong Kong, India, Mexico, New Zealand, Singapore, the UK and the US.

We would like to thank the following experts for their time and insights:

- Simeon Fishman, executive vice president and CRO at The Clearing House
- Sophie Heading, global risks lead at the World Economic Forum
- Dr Witold J Henisz, vice dean and faculty director of the Environment, Social and Governance Initiative of the Wharton School

The briefing paper was produced by a team of Economist Impact researchers, editors and designers, including:

- Monica Ballesteros—project director
- Durukhshan Esmati—project manager
- Kathleen Harrington—analyst
- Alasdair Ross—writer
- Amanda Simms—editor
- EMC Design Ltd—designer

Economist Impact bears sole responsibility for the content of this report. The findings and views expressed herein do not necessarily reflect the views of our sponsor, partners or interviewed experts.

Foreword by Iron Mountain

Over the past three years, many organisations have undergone significant transformations in response to emerging threats and global disruptors. This evolution has required all of us to become more resilient, moving away from reactive measures and towards proactive anticipation. By building resilience against potential future threats rather than merely responding to familiar ones, organisations are capable of adapting to unforeseen risks and seizing emergent opportunities.

For over 70 years, Iron Mountain has empowered customers around the world to mitigate risks to their brand, reputation, financial status, and ability to serve their customers, patients, or citizens effectively. We help protect against loss of data, vital information, and historical archives in any format; provide secure destruction of physical and IT assets; recommend policies to ensure compliance with regulators; and offer secure facilities to store inventory and precious artifacts—all within a trusted chain of custody framework. .

As you'll discover in this report, more than 90% of organisations are placing increased emphasis on risk management because of recent global and economic disruptions. In terms of emerging risks, the report highlights sustained concerns over cybersecurity. Another is the proliferation of emerging technologies, with generative artificial intelligence, for example, creating new risks and expanding risk managers' capacity to spot these threats at the same time. While protecting physical assets remains crucial to our organisation, we recognise that everyone is now more vulnerable to cyber threats, and we have moved with the market to protect customer data in a digital space.

The report findings also show that executives are paying more attention to environmental risks than they have in years past. When it comes to sustainability, our path to net zero focuses on reducing energy use, electrifying our systems and vehicles, installing renewable energy systems, and procuring green power to reduce exposure to rising fossil fuel prices and local emissions regulations. By pursuing our own environmental, social and governance goals and supporting our customers in achieving theirs, we not only mitigate the risks associated with evolving regulations, climate change and social inequality, but also unlock new opportunities.

We're heartened by the survey results showing that executives are more proactively managing risk and building resilience. This itself is at the core of our mission. The data-driven insights in this report give us a closer look at how we can better prepare ourselves and our customers for the future.

Larry Jarvis
SVP, Chief Information Security Officer
Iron Mountain

Executive summary

Risk management has become increasingly embedded in organisational structure and is represented at more senior levels. Risk managers gather data on potential threats and co-ordinate the organisation's response. But as those threats evolve at an accelerating pace, it is critical that the discipline moves towards anticipating the risks that are not yet on the organisation's radar rather than simply responding to events as they happen.

Economist Impact, sponsored by Iron Mountain, conducted primary research to understand how executives perceive the key internal and external factors shaping an organisation's approach to risk and the role that executives, technology and the institutional set-up play in risk management. Economist Impact leveraged data from expert interviews and a bespoke survey of 656 executives across key industries (financial services, healthcare and life sciences, energy, and the public sector) in Australia, Brazil, Canada, France, Germany, Hong Kong, India, Mexico, New Zealand, Singapore, the UK and the US.

Risk managers are moving towards a deeper understanding of how risks cascade through the organisation—for example, how a shutdown or security breach at a key supplier could affect their operations, revenue and reputation. Awareness of contingent risk is rising, but there is still room for improvement.

Holistic and anticipatory risk management that responds to emerging threats needs to be led from the top of the organisation, with a systematically co-ordinated risk response that is embraced and 'owned' by every staff member. Beyond the organisation, risk awareness should be embedded among partners, suppliers and distributors.

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. These evolving technologies need to be monitored carefully as their true implications become clearer.

We look at four areas where evolving practices are transforming the risk management landscape:

Workplace evolution: an organisation's staff is both its greatest asset and its biggest vulnerability, reflected in the efforts and resources that organisations dedicate to recruiting, retaining and training workers. Digitalisation has placed staff closer to critical processes, increasing risk and accelerating the pace at which it manifests. Meanwhile, the shift towards home working has made the digital boundaries of the organisation more porous. Attracting and retaining staff is also becoming more challenging as a generation embraces a more values-led approach to work. Our survey suggests risk managers are keeping abreast of these emerging trends; 96% of survey respondents indicate that their organisation has developed new workforce management policies and procedures, including hybrid work, for instance.

Cybersecurity and data governance: digital computing has not only underpinned a new wave of productivity gains, but also created new sources of risk. Information flows faster and more broadly than ever before and, critically, faster than human reaction. With contingent risk also growing through the emergence of giant, dispersed and multinational organisations, protecting an entity's digital presence from accidental or malicious harm has become a matter of survival. The launch of open generative AI models has brought a long-anticipated risk suddenly over the horizon and into the boardroom, but the impacts of this nascent technology remain hard to foresee. Managers can best respond to this shifting environment by focusing relentlessly on three major data risk areas: governance, security and privacy.

Sustainability: climate change threatens our future, but its effects are already with us. Extreme weather is becoming more intense and frequent, while biodiversity is under rising stress. There are also catastrophic impacts on trade and infrastructure, and, as such, organisations are focused on maintaining diverse and flexible supply chains. While they focus on resilience, they are also coming under pressure from stakeholders to help address the underlying problems: resource depletion, environmental degradation and dangerous emissions. Failure to act on these issues could have severe repercussions. This is acknowledged by the vast majority of our survey respondents, with 80% highlighting the importance of reputational risk indicators.

Operational efficiency: while organisations contend with a rising tide of risks emerging beyond their walls, risk managers must continue to focus on threats closer to home, whether the source is people, processes or regulatory requirements. Organisations have fallen into the trap of perceiving the risk function as a cost centre that places hurdles in the way of making money. Risk managers have become better at providing management with metrics that balance the costs of maintaining sound risk practices with the potential losses arising from dropping the ball. How operational risk manifests varies greatly among organisations and sectors, but our survey suggests that risk managers across the board recognise the importance of investment in this area.

While the risk management discipline is evolving in tune with the changing threat landscape, it continues to face considerable challenges. Among these are:

Measurement: while the costs of deploying a risk management system are clear, the same can't be said for measuring its benefits. Part of the function's role is to ensure that potential threats do not materialise, but assessing the cost of something that did not happen is problematic. And while the investment is immediate, the benefits may accrue over the years, adding to the measurement challenge. The key is building metrics that tie risks to measurable organisational objectives.

Resourcing: organisations tend to fund the risk function to reflect the landscape of the past rather than equip it to prepare for the future. At a time when new risks are emerging and old ones evolving, this tends to leave the risk management effort underfunded, undermanned and, potentially, under-skilled.

Coordination: a forward-looking, efficient and resilient risk function requires unique awareness and co-ordination throughout the corporate structure rather than in traditional siloed functions. It requires both top-down leadership and bottom-up collaboration and execution, and it should extend beyond the organisation to include its partners, suppliers and other stakeholders.

Introduction

There are no certainties in organisations' operations. The possibility that something will go wrong within each organisation and at every point along its value chain is ever-present. From a downturn in key markets to disrupted critical supplies to the malicious actions of a disgruntled employee, risks that are hard to anticipate, or avoid, create a drag on organisations' bottom lines and objectives. The damage can vary from a minor irritant to even bankruptcy and jail terms in extreme cases.

Staving off these threats is a sophisticated and fast-moving discipline. It is complicated by the fact that risks change over time in their intensity, nature and scope. During and immediately following the financial crash of 2008–09, the risk of being cut off from credit was a key concern. During the covid-19 pandemic, the focus was on business continuity as lockdowns forced organisations to close their doors. As Russian tanks rolled into Ukraine in 2022, restrictions on global food and fuel supplies drove prices skywards and roiled supply chains.

The rise of increasingly advanced, and easily accessible, forms of technology, combined with working from home becoming increasingly widespread and entrenched, has introduced a new layer of risk. The geographical boundaries of organisations have expanded from purpose-built and centralised offices to the attics, studies and garden rooms of private residences, often many miles from HQ and frequently in a different country. Securing processes and proprietary data in such a dispersed environment is doubly challenging, turning every employee into a potential point of leakage or sabotage.

Economist Impact, sponsored by Iron Mountain, conducted primary research to understand how executives perceive the key internal and external factors shaping an organisation's approach to risk and the role that executives, technology and the institutional set-up play in risk management. Economist Impact leveraged data from expert interviews and a bespoke survey of 656 executives across key industries in Australia, Brazil, Canada, France, Germany, Hong Kong, India, Mexico, New Zealand, Singapore, the UK and the US.

Risk management—trends and perceptions

Risk management has evolved as a discipline to confront evolving threats. It has moved gradually deeper and higher into an organisation's structure, involving more people and resources (though reportedly never enough) at a more senior level. Responsibility for risk is frequently held at the board level, with chief risk officers (CROs) reporting directly to the CFO or CEO. At the same time, risk managers are seen less as heads of a distinct division and more as co-ordinators of activities spread across the organisation. Ownership of risk and the responsibility for reporting it up the chain frequently belongs with divisional heads, with the risk function providing guidance, collating data and recommending remedial action to senior management.

The journey from risk as a barely acknowledged backwater to today's enterprise-wide risk architecture has been a long one. Awareness of risk as an existential organisational concern emerged in the second half of the last century, yet the first CROs weren't appointed until the 1980s, with the role not considered a mainstream response to risk until the early years of this century. Today, risk management is acknowledged as a key competency of senior management. More than four in five organisations represented in our survey report investing in enterprise-wide risk management teams as part of their tactical approach to the discipline.

Our research suggests that the journey remains incomplete, although senior risk managers are becoming increasingly sophisticated in understanding the discipline. For example, attention is shifting from reacting to risks as they emerge to anticipating them and building resilience into the organisation before damage occurs. Identifying risk has risen in importance for more than 90% of our respondents since 2020, as has predictive risk modelling for nearly as many. The focus on anticipation extends to reshaping the organisation for that purpose, and 28% report seeking an improved ability to identify and anticipate threats, while 41% say they anticipate risks by monitoring emerging threats and identifying process anomalies. This shift in focus is hardly surprising given the succession of shocks that have blindsided organisations' managers over the past few decades.

Organisations are also grappling with the interconnectedness of risk. An adverse development in one part of the organisation, or the world, can cascade through the operation in myriad ways. If a key supplier is shut down through a natural disaster, this can lead to production delays, increased costs as alternative supplies are sought, lost revenue as orders are delayed or go unfilled, and a blow to the brand and the organisation's reputation as news of the disruption circulates. From a single third-party risk, the entire organisation is drawn into crisis management. Anticipating these contingent threats is a key element of modern risk management.

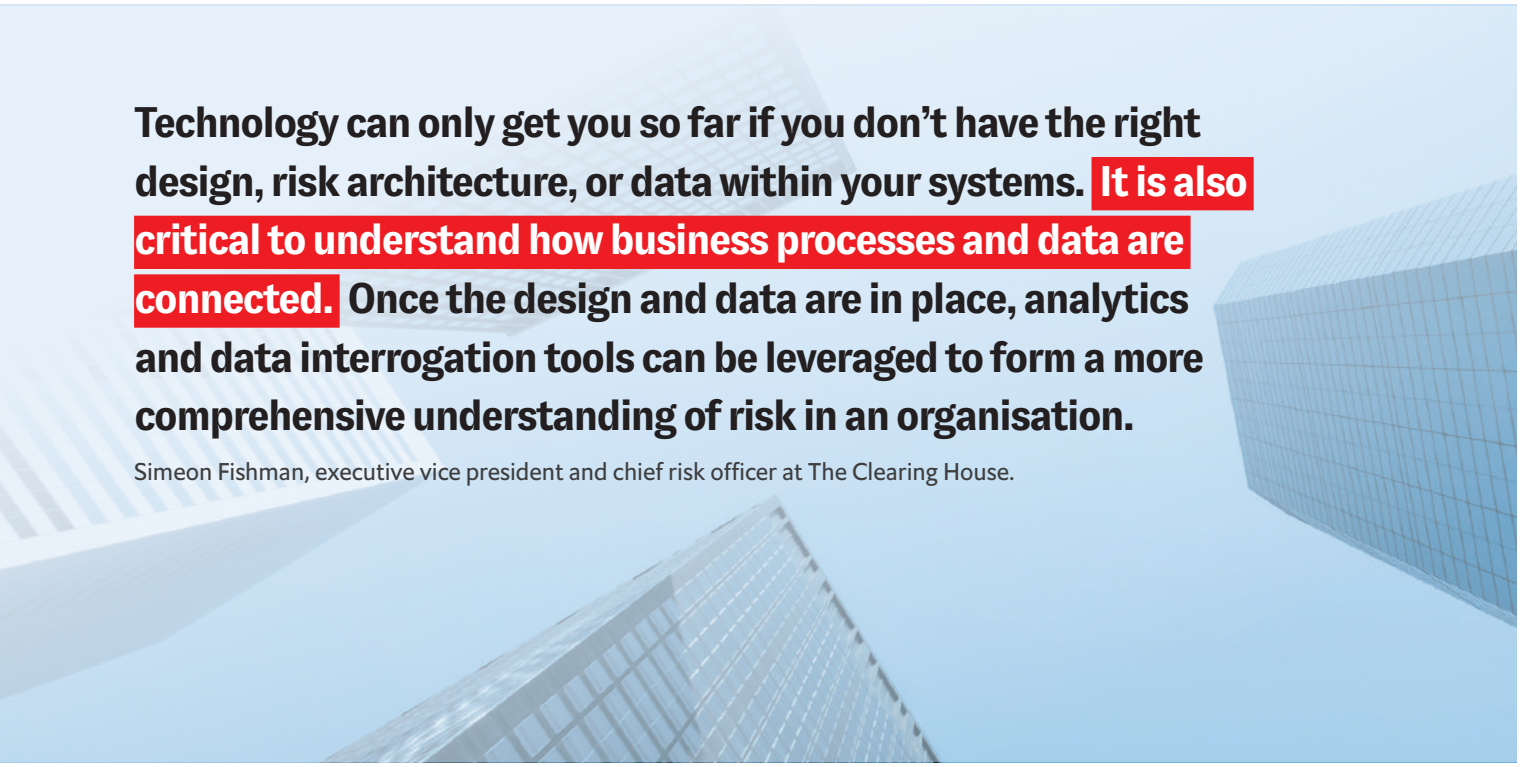
Again, organisations are making progress, but there is room for improvement. Sophie Heading, global risks lead at the World Economic Forum, explains that "there is a better appreciation of connectivity between risks, but it is still evolving. Using a bit of imagination, the implication of events on one side of the world can be used to foresee a potential risk on another. The lack of such a view may make the organisation susceptible to risks that arise from these events."

Simeon Fishman, executive vice president and CRO at The Clearing House, believes there is increasingly more focus on emerging risks, ie, risks that are less defined and apparent. He explains that "now it is more critical for organisations to get greater visibility on the horizon and attempt to understand these risks better. One crucial area of emerging risk is technology risk which is continuously evolving. For example, only a few vendors provide cloud services, which has the potential of resulting in cloud concentration. A tech-centric organisation, through the software they use or develop, may unwittingly put all their eggs in one or just a few baskets."

Managers are aided in this transition from reactive to proactive risk management by an emerging suite of digital tools, as reflected by the responses to our survey, where 43% of executives reported using cognitive technologies and AI to manage risk. However, while change is the stock in the trade of risk managers, change at the pace we're observing in AI brings its own challenges. It is clear that machine learning offers a new way of interrogating the data that flow in and out of a large organisation, assisting human analysts by spotting patterns they might not see. But it may also prove a vector for cyberattacks as hackers and scammers use the technology to supercharge their programming. The simple fact is that it's still too early to say how this technology will develop and its net impact on risk management.

The need to anticipate risk and its impacts throughout the organisation at a time of rapid technological change emphasises the importance of adopting a holistic approach to risk management. Relying on reacting to threats once they materialise leaves organisations wrong-footed and struggling to catch up. Focusing separately on each area of the operations exposes the organisation to contingent risks. The answer is not simply to rely on innovative technologies. Blindly embracing innovation leaves organisations open to new and unforeseen threats. Ms Heading cautions that "technology enables risk management. But it needs to marry with the human element."

The holistic approach to risk management requires leadership from the top and co-ordination down and across the organisational structure to bring all the available information to the attention of those best placed to interpret it and act. Dr Witold J Henisz, vice dean and faculty director of the Environment, Social and Governance Initiative of the Wharton School, concurs with this, adding that "making data comprehensible, transparent and easy to understand is extremely important when bringing people of different data skills and functional backgrounds together."



Technology can only get you so far if you don't have the right design, risk architecture, or data within your systems. 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 organisation.

Simeon Fishman, executive vice president and chief risk officer at The Clearing House.

As the 'holistic' label suggests, risk management is becoming the responsibility of the entire organisation (and its suppliers, partners and distributors). Risk managers implement and co-ordinate the system, but unlike the marketing director or the operations manager, this is not a competence reserved solely for them. Evolving from an office embedded somewhere in the organisational chart, risk management has become an integral element of organisational culture, alongside its brand, mission statement or approach to developing and retaining human capital. It includes organisation-wide commitments such as a risk appetite statement, an increasingly common feature of modern organisations that defines the level of acceptable risk and its overall risk-taking attitude.

Central to this approach is co-ordination between the various units of the organisation, its extended supply chain and its key stakeholders. Many senior risk managers are champions of this approach within their organisations, as our survey shows. Among respondents, 77% agree that risk management must consider all parts of the organisation, while 46% report investing in enterprise-wide risk management teams. A further 36% report integrating risk management into overall organisational strategy and decision-making as a priority. This requires "structural changes that vary with the type and size of the organisation," according to Mr Fishman. "Communication from senior leadership and the CEO down to everybody becomes more critical in ensuring that risk management is part of the DNA of the entire organisation and not just a carved out function that assumes special ownership of driving risk management."

But executives still fall short of achieving the ideal situation. Fifty-seven percent reported that their organisation needs to improve their cross-functional collaboration. Only 4% of surveyed executives reported having a risk management committee that is directly responsible for driving risk management, while 27% said that their CEO/president/partner is directly responsible. Over 60% of respondents think their organisation needs to improve employee engagement and information sharing between functions, teams and external partners.

Risk management in the four pillars

By its nature, risk is diffuse. Even when the sources are clear (a rare occurrence), the route risk takes—where it enters the organisation and how it travels through it—is hard to predict. In this section, we'll look at four distinct manifestations of organisational risk, track their effects and explore how managers address them. The four pillars are:

- Workplace evolution
- Cybersecurity and data governance
- Sustainability
- Operations efficiency

Workplace evolution

An organisation is little more than the group of people it brings together to pursue its mission. Their varying talents combine to turn inputs into outputs of a higher value. Rightly, many organisations value their human resources extremely highly and invest money and effort into recruiting, training and retaining them. However, along with their skills and energy, humans come with unpredictability and a tendency to make mistakes. People risks are some of the most difficult to manage for three reasons. First, they mediate every process an organisation performs with or without technology, so the risks they pose manifest everywhere. Second, they are subject to human drives, resulting in an unpredictable performance compared with that of a machine. Third, the relationship between organisations and their staff is evolving, with remote working becoming more commonplace, so what prevails today may be different from tomorrow.

People have always been organisations' greatest strength and biggest vulnerability, but recent developments have added to the risks. The digital transformation over the past few decades has boosted productivity in general, but it has also brought employees closer to mission-critical processes and valuable data. Because of this proximity, careless or ill-intentioned staff can cause more damage quicker than ever before. More recently, the covid-19 pandemic forced a profound and sudden transformation of many work environments, leaving organisations short-staffed at a critical time and rushing to set up working-from-home systems.

This also presented organisations with a novel managerial challenge, as Mr Fishman explains. "We may not have the same understanding of everyone's roles and responsibilities—getting visibility into everyone's behaviours and some risk vulnerabilities get more challenging with remote work," he says.

As the pandemic subsides, organisations are finding that their employees' attitudes to work have changed, perhaps permanently. Existing staff are often unenthusiastic about returning to the office, while potential new recruits expect some element of home working as standard. Organisations have also experienced a dearth of labour, partly through the long-term health impacts wrought by the pandemic, but also through a trend dubbed 'the great resignation', which was caused by a confluence of factors such as protesting toxic workplaces.

In the future, generational changes in the attitudes and expectations of employees, including an increasing prioritisation of values such as diversity, sustainability and social justice, will make attracting and retaining staff more difficult. Salary alone won't be enough. That will threaten to create a mismatch between the skills required in a fast-changing technological environment and the availability and willingness of recruits in the marketplace. Organisations may find themselves operating with a skills gap, undermining productivity and increasing the risk of mistakes and malicious acts.

As in other areas of risk, not all organisations are keeping up with developments, although many are. The most innovative are relocating offices to adapt to the new, more decentralised reality. Our survey results show that 94% of organisations have diversified their approach to the physical office and workplace, with the pandemic prompting 45% of them to do so in the last three years. In keeping with this, 96% of survey respondents have indicated that their organisation has developed new workforce management policies and procedures, including hybrid work. Organisations are also assessing talent requirements for a changing world of work, which includes the risk function. Leading organisations are "looking at the staffing model within their organisation to ensure they have technologically competent risk managers," says Mr Fishman. "The role of technology subject matter experts in risk and recovery is critical, such as cloud and AI experts."

Organisations are also gathering more data on workforce-related issues and developing more systematic processes for managing recruitment and retention. Our survey backs this up, with half of the respondents saying they are leveraging more data to do so, with slightly more reporting they have developed a talent pipeline.

Cybersecurity and data governance

Organisations' enthusiastic embrace of information technology has transformed their operations. From the old days of centralised facilities with armies of workers overseen by austere managers in strict hierarchies, organisations have become looser, more agile and far more productive, thanks largely to digitalisation. Computers, automation and the internet have disrupted working models profoundly, and future developments such as quantum computing, an all-pervading Internet of Things and the metaverse promise equally fundamental change.

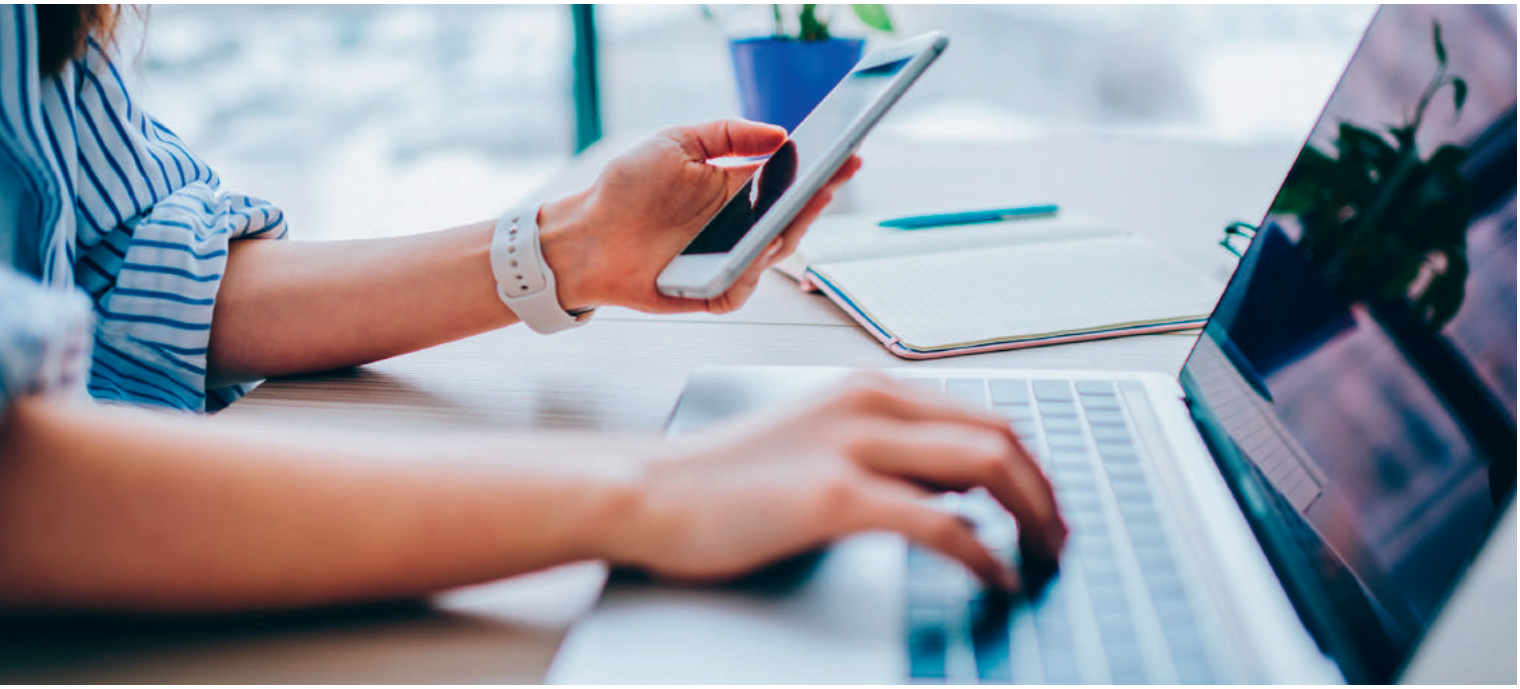
Broadly speaking, the impact of the digital revolution on organisational risk management has been threefold: risks emerge more suddenly and spread a lot faster; data, its storage, transmission and interpretation, has become a mission-critical ingredient in operations; and, while digitalisation has created new areas of risk, it has also given rise to new tools with which to address it.

When information travels at the speed of light across a global digital network, things change faster than a human can react. With computers increasingly making decisions on humans' behalf, processes can advance through numerous iterations before an error or unintended outcome is spotted. With clients, partners and customers all plugged into global communication media, a brand's reputation can find itself in the court of public opinion before the organisation's executives have fully absorbed what's happening.

With generative AI, we are seeing a new potential cyber risk emerge. The pace of its adoption has left society in its wake, with policymakers and regulators—and the technology's pioneering creators—struggling to keep up. Risk managers are unsure where to turn for the best advice at this early stage of what could prove as disruptive to business models as the internet itself. "Who has risk expertise on where generative AI is going?" asks Mr Fishman. "What sophisticated ways can we adopt to monitor cloud concentration better? Given how the cyber landscape changes, how can we continue to embed resiliency in our infrastructure and processes?"

This area poses pressing questions and complex challenges for risk managers and organisations. At such times, covering the basics is a good place to start. It remains paramount that organisations focus on three major areas of risk when it comes to managing their digital assets:

- Data governance: ensuring the accuracy, consistency and accessibility of data.
- Data security: protecting data from unauthorised access, use, disclosure, disruption, modification or destruction.
- Data privacy: protecting the privacy of individuals by controlling how their personal data are collected, used and shared.



The same principles of proactivity and horizon scanning continue to hold but with more urgency than before. Similarly, ensuring compliance is more of a challenge in such a fast-changing and uncertain regulatory landscape, but no less vital.

Our survey results indicate that organisations have shown dedication and consistency in their efforts to mitigate data and cybersecurity risks through different measures. Over the past three years, 49% of organisations invested in disaster recovery/business continuity plans for digital systems, and 48% invested in cloud services/ storage and ongoing monitoring and prevention of cyber risk and threats. During the same period, investments in IT and cybersecurity talent, and training on data/technical literacy have also been reported by 46% of surveyed executives.

Meanwhile, risk managers should take a keen interest in the evolution of AI, not just as a source of risk but also as a means of mitigating it. Forty-three percent of our respondents report using cognitive technologies and AI in risk management processes. Properly trained and directed, AI can detect odd patterns, identify trends, plot scenarios and spot areas of risk that human analysts might not see.

Few organisations are free of cyber risk, but some sectors are more prone than others. For example, the healthcare and finance sectors both capture huge amounts of sensitive customer data. Getting the best use out of this trove of data, not least as a route to calculating risk either to the client or the organisation, all the while keeping it secure, is a mammoth task. The costs of failure can be devastating. Unsurprisingly, among all industries, the healthcare sector had the highest percentage of survey respondents, at 83%, indicating the growing significance of technology indicators over the past three years. These included network uptime, cybersecurity incidents and software errors.

The energy sector similarly relies on data to streamline its operations, while the modern state leans heavily on citizen data to provide public services with maximum efficiency. In the case of governments, the reputational costs of failure can be particularly damaging, bringing politicians and their parties into direct conflict with those who vote for them.

Sustainability

Industrialisation has brought boons to humanity unimaginable to our pre-industrial forebearers. But by burning fossil fuels to power it, we have put the sustainability of our lifestyle—and our lives—at risk. Greenhouse gases (GHGs) released into the atmosphere, largely because of our economic activity, are raising average global temperatures. The effects will be potentially catastrophic over the coming decades, but we don't have to wait that long. Extreme weather events are increasing, sea levels are rising and biodiversity is under stress.

This impinges on organisations in two ways. First, operations and supply chains are vulnerable to disruption through extreme weather events and other environmental effects that are hard to anticipate. The events of the past three years have made 47% of surveyed organisations focus on maintaining diverse and flexible supply chain networks. Second, organisations' stakeholders, from customers to investors to employees, rightly expect entities to pull their weight in addressing resource depletion, environmental degradation and GHG emissions.

For now, the second is more pressing for risk managers (though the former is a growing threat). Activist groups quickly single out what they consider egregious offenders against sustainable practices, with a growing arsenal of creative means for drawing public attention. Oil and energy companies and the investors and banks that finance them have come under persistent attack. Such campaigns can disrupt business operations directly but can have a more pernicious impact by undermining an organisation's reputation and 'social licence' to operate.

The importance of reputational risk indicators among executives has grown in recent years due to the increasing complexity of the operating environments and the need for organisations to be more transparent, accountable and socially responsible. A significant 80% of our survey respondents identified reputation risk indicators as the most crucial in terms of the growing importance to their risk monitoring.

As with cybersecurity, sustainability and the associated areas of social policy and governance (ESG) is a fast-changing risk landscape. Environmental concerns have gained prominence on the public agenda, with organisations responding by issuing statements advertising their 'green' credentials. However, such statements are frequently dismissed as 'greenwashing' and insufficient to insulate organisations from public anger. Green mission statements have increasingly been superseded by pledges to achieve 'net zero' GHG emissions, accompanied by roadmaps to show how this will be achieved.

For larger organisations, this is no longer enough. Citizens are pressing for a 'nature-positive' stance from the corporate and public sectors, with organisations pressed to lay out plans for restoring the environment to its pre-industrial state, or at least to bring climate indicators back within limits compatible with a sustainable economy. Ms Heading points to "a shift in risk management from looking simply at regulatory compliance, particularly as a tick-the-box kind of exercise, towards a far more strategic function, incorporating societal values such as ESG."

Our survey reflects the fact that ESG now appears on organisations' risk registers. Nearly half of the surveyed organisations dedicated more resources to ESG initiatives, while a similar number focus on ESG performance reporting—which is required by regulators in some jurisdictions.

Operational efficiency

Closest to home for organisations and their risk managers is their internal operations. Most can do little to influence circumstances beyond their walls, physical or virtual, but what happens within is mostly under their direct control. Whether people, processes or regulatory requirements, the efficiency of an organisation's inner workings is the difference between success and failure. And it is fraught with risks: staff can fail to perform as expected, be let down by the equipment they rely on or fall foul of vulnerabilities in the processes designed to make them collectively productive.

Guarding against such risks has been a central feature of risk management since the discipline's first days. As such, risk managers can easily fall foul of old perceptions of being little more than an internal police officer placing obstacles in the way of other departments. The risk function therefore comes to be viewed as a cost centre and a burden on the enterprising drive of the 'money-making' verticals. This perception was (and sometimes still is) a millstone around risk managers' necks, but things are changing. Risk managers have gotten better at measuring the costs of operational failures and stacking them against the cost of maintaining a fit-for-purpose risk function. Compared with suspending operations to restore a failing process, a hefty regulatory sanction for mishandling customer data or losing business due to a well-publicised ethical failure, the cost of an agile risk management function is less onerous.

No two organisations are alike, so there is no blueprint for achieving operational efficiency. Indeed, what is meant by 'operations' can vary greatly within and between organisations. The energy sector focuses on equipment and processes, as drilling for oil or extracting minerals is highly capital intensive and failure can cause human and environmental disasters. The financial sector is both data-heavy and vulnerable to failures among its staff through illegal breaches of policies and roles, poor execution, lack of training, and unethical behaviour. These can result in direct losses as well as regulatory, legal and restructuring costs. Legal and regulatory compliance is particularly important, complicated by the fact that many banks and financial institutions operate across multiple legal jurisdictions. Other industries vary in the focus of their operational risk management—one of the many factors complicating the job of risk managers.

Our survey reflects the importance of operational risk to organisations, with a clear sense that investment in this area improves performance and financial results. Most notably, 42% of respondents report an improvement in performance resulting from the application of good management practices in facilities and physical workspace planning. A similar percentage report a significant improvement in their organisation's operational efficiency. However, two-thirds of respondents recognise that this is a long-term play, and that the investment in risk management disrupts operations in the short term.

Dr Henisz says that recognising the connection between investment and return is critical. "We can monetise risk impact by calculating days of shutdown and lost production," he says. "Translating the data into the language of finance or operations is critical. Otherwise, the risk management function will only be seen as a cost while everyone else drives revenue."

Challenges to risk management

The risk management profession has become more influential and sophisticated over time and is embedded in the culture and structure of most large organisations. But its role and methodologies are under continuing pressure to keep up with a risk environment that is in a constant state of change. There has been a tendency to consider a risk strategy that could cope with every threat experienced in the past as sufficient, yet the past is often a poor indicator of how risk will manifest in future. In response, risk management must be constantly evolving as new threats and disruptors come into focus. In particular, the profession needs to continue along the journey from reaction to anticipation, building resilience against the threats to come rather than simply responding to familiar ones.

In this regard, our survey shows some progress, but suggests that there is more to be done. An overwhelming majority of surveyed executives are confident that the risk management initiatives implemented by their organisations are sufficient to mitigate or prevent damage from risk. This hints at a degree of overconfidence by organisations that could leave them more exposed than they think. Addressing this potential shortfall involves three major areas of focus: measurement, resourcing and co-ordination.

Measurement

Tracking performance in risk management is inherently tricky. If there is a failure of risk management, costs incurred may be attributed to the risk programme. This seems clear, but determining what percentage of the costs should be assigned to the function is far from straightforward. It's even harder to credit risk management when things go well. There is a tendency to consider this nothing more than 'business as usual' and to deny the contribution of risk managers altogether. Even where some effort is made to give credit to the function, quantifying what should be entered in the 'positive' column is difficult.

Should the risk function be expected to account for investments made in anticipation of risks that never materialised? Should it be responsible for black swan events (difficult to predict but in retrospect appeared inevitable) that did not surpass the threshold for attention? In the aftermath of the 2008–09 global financial crisis, widely seen as a black swan event, the risk discipline—including credit rating agencies—was shaken to its foundations. No doubt, the credit crunch was an indication of the failure in understanding and managing risk, but policy mistakes and public recklessness were also to blame. It is hard in such circumstances to carry out a forensic accounting of risk management's performance with even a pretence of precision.

Risk management also shares the difficulty experienced in many operational areas of justifying short-term investment for long-term benefit. "You invest in something today and you may not see the trade-off for five to ten years, or you might see it in three months' time," says Ms Heading. "Depending on what you're trying to put controls around, it can be very difficult to articulate that kind of cost-benefit in a way that's readily understood by executives."

Executives recognise the challenges in measuring risk management performance. Around three-quarters of survey respondents agree that the lack of standardised evaluation metrics to measure risk makes it challenging to show progress.

"Building metrics that tie risks to organisational objectives and ensuring they are clear, from work on the ground up to the board and executive leadership, is essential," says Mr Fishman. "Tools can help, but the structure of measuring risks tied directly to activities and their impact is fundamental. You need to look at not just the impact but must also understand the causal drivers. For example, although measuring cyber events are important, just as important is measuring how efficiently processes and systems patch vulnerabilities and ensure business continuity."

Resourcing

Few departments consider themselves to be adequately funded, but the risk managers' case is particularly strong. This is partly because organisations tend to fund the function to reflect the risk landscape of the past rather than equip it to prepare for the future. The breadth and complexity of risks facing organisations have been increasing steadily as supply chains lengthen and become leaner and as technology accelerates the pace of change. Similarly, organisations can avail themselves of a growing suite of tools for monitoring risk and building resilience, but they require big up-front spending and, as discussed, the timing and size of the return on investment is hard to quantify.

Survey respondents reflect the sense that risk departments are under-resourced. Executives believe that their organisation's financial, technological and human resources dedicated to risk management are insufficient, with nearly two-thirds saying their organisation needs to improve on this front.

Part of the challenge is that, as organisations become increasingly digital, risk managers must have a wider scope of expertise. This means that even to sustain a consistent level of protection, organisations must spend more to attract the required skill sets to the risk management function. "Risk managers are a hot commodity," says Mr Fishman. "Even with massive layoffs in the financial and tech sectors, good risk managers are hard to find."

With developments such as AI, automation and robotics all pressing for attention, this bottleneck is likely to get worse. Coupled with the approach of technologies such as quantum computing and distributed ledger technology at scale, there will be no room for complacency in the risk management industry for the foreseeable future.

Co-ordination

As we have discussed, a core risk management requirement in the coming years will be the ability to bring the risk mindset to all corners of the enterprise. Bottom-up information process flows need to be co-ordinated across the organisation, with risk managers establishing the rules and tools that every department and employee should use. Top-down leadership needs to set the tone so that the central role of building resilience against known and unknown threats pervades the organisational culture. Partners, suppliers and customers must be included in the network, extending the organisation's risk radar well beyond its walls. The entire risk management apparatus needs to be focused on what is happening in the organisation day-to-day, but also, and critically, what might happen in the future given emerging trends. The most successful organisations will be those in which this effort is designed and co-ordinated by top-flight risk managers, armed with the skills and resources required by a fast-changing environment and with the support of the most senior executives.

The risk management journey is not yet complete, but the direction of travel is promising.

Conclusion

Risk management has come a long way since its first manifestation as a distinct organisational function. It has evolved from a discipline limited primarily to banking, where the solution was to build more generous financial cushions to guarantee liquidity during adverse market developments, to a centrepiece of modern management. Risk managers are prominent in organisations across all industries in both the private and public sectors. They capture and quantify threats across a wide range of factors, arising both within the organisation and outside its walls, where there is less visibility and control. Risk management has been embraced at ever more senior levels of the organisation, with many risk managers today operating in the C-suite with access to the CEO or the board. This has been the direction of travel for some decades, and the function continues to become more deeply embedded.

But new challenges are emerging, and old ones are morphing as technology, geopolitics and social change affect the operating environment. Risk management has always been a dynamic discipline, but the need for change is becoming increasingly pressing. This young century has thrown up a succession of global disruptions. From the global financial crisis of 2008–09 and a subsequent crisis of confidence in liberal democracy, to the covid-19 pandemic and Russia's invasion of Ukraine, tectonic movements in world affairs have multiplied uncertainty. This has happened against the backdrop of a long-established but accelerating transition towards a digital landscape, as well as environmental concerns that are impinging on business, society, politics and the global economy.

The acceleration in digital adoption, exemplified by the emergence of generative pre-trained large language models, brings both promise and threat. While it promises to spawn a new generation of tools to help organisations monitor and respond to risk, it carries the threat of arming malicious agents with similarly innovative weapons for stealing or corrupting precious data. New working patterns, particularly the growth of home working, expand and dissolve the organisation's digital front line, opening new routes to cyber threats.

Risk managers are pressing on with the journey that began decades ago, embedding a 'risk-minded' approach to operations throughout the organisation. They are grappling with the increasingly contingent nature of risk, where an event in a remote corner of the supply chain can produce unforeseen ramifications elsewhere.

Critically, they are also transitioning from a reactive stance to a proactive one. The former approach focuses on building resilience against expected threats and responding to them when they materialise. In the latter, risk managers expend resources and effort on scanning the horizon for threats not reflected in the risk register, preparing for scenarios that may appear improbable and carry a high potential for damage.

In today's shifting risk landscape, wider, faster-changing and more complex than ever before, embracing the proactive approach may be the single most effective action the risk management discipline can take to arm itself for the future.

ECONOMIST IMPACT

LONDON

The Adelphi
1-11 John Adam Street
London WC2N 6HT
United Kingdom
Tel: (44) 20 7830 7000
Email: london@economist.com

GENEVA

Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
Email: geneva@economist.com

SÃO PAULO

Rua Joaquim Floriano,
1052, Conjunto 81
Itaim Bibi, São Paulo,
SP, 04534-004
Brasil
Tel: +5511 3073-1186
Email: americas@economist.com

NEW YORK

900 Third Avenue
New York, NY 10022
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
Email: americas@economist.com

DUBAI

Office 1301a
Aurora Tower
Dubai Media City
Dubai
Tel: (971) 4 433 4202
Fax: (971) 4 438 0224
Email: dubai@economist.com

HONG KONG

1301
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
Email: asia@economist.com

SINGAPORE

8 Cross Street
#23-01 Manulife Tower
Singapore
048424
Tel: (65) 6534 5177
Fax: (65) 6534 5077
Email: asia@economist.com