BUSINESS RISK

03 THE BENEFITS OF A BOTTOM-UP APPROACH

06 DO YOU NEED A CHIEF WORRY OFFICER?

12 THE RISKS OF INACTION ON NET-ZERO GOALS

See us on page 11

BUSINESS RISK

Distributed in THE TIMES

Published in association with airmic

Contributors

Bradley Gerrard
Business and finance journalist with bylines in the *Daily Telegraph*, *FTfm* and *Investors Chronicle*.

Tamlin Magee
A London-based freelance journalist who has contributed to a wide range of publications. He specialises in technology and culture.

Virginia Matthews
Fleet Street-trained reporter, writer, editor and columnist with extensive experience of daily news, business reporting and feature writing/editing for daily and weekly publications.

Michelle Perry
Journalist, commissioning editor and copywriter covering the business, finance and property sectors.

Jonathan Weinberg
Freelance journalist, writer and media consultant/trainer specialising in technology, business, social impact and the future of work and society.

Alex Wright
Business and financial journalist with more than 20 years' experience, having worked on international, national, regional and local papers, and trade and consumer magazines.

raconteur reports

Publishing manager
Jean-Philippe Le Coq

Managing editor
Sarah Vizard

Deputy editor
Francesca Cassidy

Reports editor
Ian Deering

Sub-editor
Gerrard Cowan
Kate Williamson
Lorraine Eames

Head of production
Justyna O'Connell

Design/production assistant
Louis Nassé

Design
Celina Lucey
Colm McDermott
Samuele Motta
Sean Wyatt-Livesley

Illustration
Sara Gelfgren
Kellie Jerrard

Design director
Tim Whitlock

Although this publication is funded through advertising and sponsorship, all editorial is without bias and sponsored features are clearly labelled. For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 3877 3800 or email info@raconteur.net

Raconteur is a leading publisher of special-interest content and research. Its publications and articles cover a wide range of topics, including business, finance, sustainability, healthcare, lifestyle and technology. Raconteur special reports are published exclusively in *The Times* and *The Sunday Times* as well as online at raconteur.net

@raconteur /raconteur.net @raconteur_london

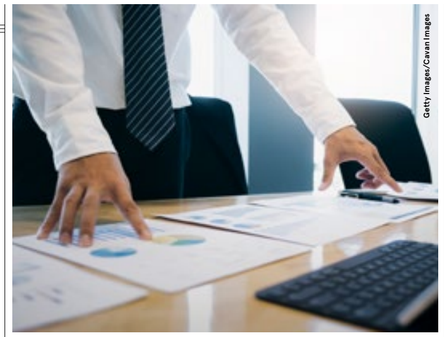
raconteur.net /business-risk-2022

STRATEGY

Managing corporate risk from the bottom up

Risk management has traditionally been viewed as a leadership role. However, spreading responsibility across the organisation can help the bottom line and improve customer outcomes

Jonathan Weinberg



Getty Images/Cavan Images

The traditional approach to risk management puts managers and the senior leadership team in the driving seat, charging them with predicting, identifying, avoiding and containing risks. But could a bottom-up mindset prevent more issues from occurring in the first place?

Many companies are increasingly offering all their employees a greater degree of training and responsibility for risk management. Progeny, an independent financial planning and asset management company, has adopted this approach. Chief risk officer Charlotte Willis believes risk management and reporting is everyone's responsibility, a way of working that can lead to the quick and effective implementation of actions and problem-solving.

"As staff have invested time and energy into helping shape strategies and action plans, their engagement and accountability is almost always assured from the outset, compared with a top-down only approach," Willis says.

Each business area within Progeny has initial responsibility for identifying and quantifying risks using a risk management framework. However, significant work has been undertaken with team heads to help them understand how their decisions affect the whole company, as well as their own specific areas.

Along with heads of departments, they can escalate new or emerging risks to a risk and audit committee, which itself works with the CRO, senior leadership team and executive board to prioritise these risks.

When teams accept and agree responsibility it also means greater alignment in pursuing new strategies or business goals, Willis adds. However, establishing a consistent approach to risk management is a challenge, she admits.

"Some departments are naturally more opportunistic and entrepreneurial, whereas others are maybe more naturally governed and risk averse. This places greater importance on the formalising of requirements and responsibilities for all staff," she explains.

It will always be up to an individual risk officer to decide if a bottom-up approach is suitable for their company and industry. For Michael Brown, health and safety content manager at compliance firm Citation, it brings a number of advantages in health and safety management, given employers have a legal duty to consult with their employees or representatives on such matters.

"Employees themselves can often offer solutions that are overlooked by management by virtue of being more familiar with how work is actually completed," he says.

Such a path can also mitigate risks when new processes or equipment are implemented in the workplace, ensuring any concerns are not ignored, according to Brown.

"Consultation in these instances helps to identify potential risks and hazards with a new process before it's fully up and running. This can help save time, effort, money and, most importantly, possible injuries from potential misuse of the equipment down the line," he explains.

In financial services, risks can be acute. Dr Luke Carrivick is deputy executive director at ORX, a member organisation for operational risk professionals in financial services. He thinks a bottom-up approach is a "great way of making the actual risk takers think more clearly about what they do".

However, he points to a downside: an overly narrow focus on information by individuals or teams can mean some broader risks are missed. For example, ensuring the aggregation of similar risks, which in isolation might be immaterial, but in combination could be important.

A more contemporary approach is now being used, akin to crowdsourcing, Dr Carrivick explains. This involves polling a diverse set of individuals on a particular topic within or even across institutions. In cases where people don't know what to monitor or be on the lookout for, what he describes as "noisy information from a range of sources" needs to be collated when identifying new or emerging risks.

"Some banks are piloting the crowdsourced concept," he explains. Industry studies such as ORX Horizon are built on this principle, he notes, with the latest version identifying emerging technology as the financial services industry's most concerning and problematic emerging operational risk.

Risk management is also becoming increasingly digital, with the digitalisation of finance occurring alongside the automation of previously manual processes.

"By embedding risk management into the business-as-usual process and by being increasingly reliant on metrics that can be automatically captured, this bottom up, data-driven monitoring of activity then begins to drive your understanding of your risk profile," Carrivick adds.

It's important to recognise that employees on the ground are closest to the operation and have "a wealth of experience and knowledge on what causes disruption", believes Julie Goddard, a business continuity consultant at Databarracks, which provides IT disaster recovery and business continuity services. "They also tend to come up with creative and clever solutions, because they're probably doing it already as part of their day job," she says.

Goddard also notes the importance of developing trust within the hierarchy, so employees know their views are valued, while management must agree the thresholds within which they would be happy for staff to manage risks themselves. This could be based on their company's risk appetite, and be a cost value, the number of customers affected, or the extent of disruption. Above the set level, issues would then be escalated.

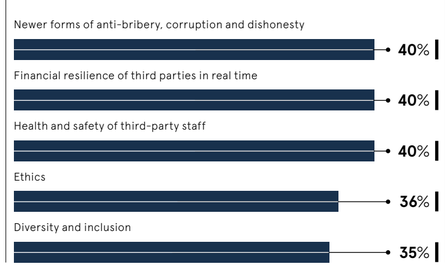
A bottom-up approach to risk management should now underpin business strategy and opportunity, Willis advises. "The more engaged everyone within the firm is with what all too often is a challenging subject, the better it is for everyone," she says.

"Risks can be reduced and opportunities can increase, both of which can have a really positive impact on business growth and a firm's bottom line, while improving customer outcomes and delivering an outstanding client service."

To achieve this, CROs could always follow a simple piece of advice from Goddard. "If you are brave enough, put a sign on the mirror in the loos saying: 'You are looking at the organisation's risk consultant'."

A MORE BOTTOM-UP APPROACH TO RISK MANAGEMENT COULD HELP BUSINESS ADDRESS EMERGING RISKS Deloitte, 2021

Percentage of companies which say their understanding and awareness of the following emerging risk domains is lowest



Commercial feature

Navigating the shifting business risk landscape

As the business risk landscape continues to shift, now, more than ever, businesses should consider their insurer less as a last resort and more as a trusted adviser. Developing a long-term relationship can provide the added value, insight and risk management that is invaluable at to help protect their operations

Risks are all around. The principal risk is, of course, the risk to the executives of an organisation. The directors and officers of a business shoulder the greatest responsibilities and face personal and corporate liabilities if they make the wrong decisions.

"In the last five to 10 years, there has been a major shift in the application of director and officer liability (D&O) insurance cover," says Catherina MacCabe, focus group leader international management liability at Beazley. "Once reserved for financial problems arising from the need to restate earnings or profits, there are many more event driven D&O claims made today."

ESG and reputational risks go far beyond concerns about climate change. Today the diversity of board members, claims about greenwashing a firm's green credentials, mismanaging the firm's adherence to ever changing regulations and governance requirements and the personal and financial conduct of senior executives all fall under D&O risk, and can result in costly disputes and litigation.

Employer risks, covering everything from how you recruit, reward and retain staff are also under close scrutiny – not only from business analysts, but shareholders, regulators, lobbyists and employees.

Every risk is also a reputational risk with the potential to not only disrupt the business in the short term, but to cause permanent damage.

"This is where insurers with a depth of experience and claims data insight can help. By sharing their vast experience of risk to identify not only where businesses experience losses, but also to help identify the specific risks within a client's organisation, and tailor D&O cover to suit their needs" says MacCabe.

Understanding the business mindset

Specialist insurer Beazley's annual risk & resilience report asks C-suite directors to identify the key risks they believe threaten their business. The list includes supply chain instability, business interruption, boardroom risk, crime and both reputational and employer risks.

Employer risk was considered to be a key concern in 2021 by 11% of respondents. They also predicted it would remain the same for 2022, but it has actually increased dramatically in the last 12 months, with almost a fifth (19%) now considering it a major concern.

Some of this may be associated with reputational risks from ESG concerns. ESG was a new entry into Beazley's questionnaire for 2022, it jumped up the agenda for 18% of those surveyed.

According to Beazley's research, boardroom risks have remained a high priority for many business leaders. Cyber risk has, rightly, become a primary concern for business leaders, and the impact of a cyber breach is not only increasing each year, but becoming more expensive to resolve. This is because cyber threat actors are becoming more aggressive in their exfiltration of target's data and are looking at more inventive and aggressive ways to extort money from their targets.

The Covid-19 pandemic forced organisations to open up their systems in ways that they had never envisaged in order to permit employees to work remotely, says Raf Sanchez, head of cyber services at Beazley. "This sudden shift to homeworking meant organisations had to implement remote access to business systems often before they had the time to understand and mitigate the risks this entailed" he says. "Some businesses rolled out training and adopted additional security measures such as multi-factor authentication (MFA) but many had neither the resources nor the budget to ensure these measures were implemented in time. Optimism about business risk does not equate to mitigation."

> Every risk is also a reputational risk with the potential to cause permanent damage

Ultimately, adopting new technology practice is only part of the process of building business resilience and reducing the threat of cyber risks.

Cyber risk cannot be ignored

One of the greatest misconceptions about cyber risk is a belief that attackers only want access to high-profile, blue-chip companies, Sanchez says. "The reality is that just like in any marketplace, we see attackers that specialise the mass-market and who can deploy automated attacks with almost zero cost (or risk of being caught) against any business or organisation regardless of size or sophistication," he adds. "Businesses that find their operations disrupted are as likely to be small enterprises or even sole traders as a multinational bank or entertainment company."

The risks, and therefore the impacts, are not contained to just financial considerations. They are operational, financial, legal and reputational. Data exfiltration raises trust issues with clients and employees, data unavailability results in immediate operational impact and organisations may be under contractual duties to notify their clients of cybersecurity incidents that can result in automatic termination of customer contracts.

Since many attackers use extortion, specifically the threat of publicising the cyber attack, as a lever to encourage payment, it can be tempting for organisations to consider paying off the criminals, but this comes with its own risks, Beazley argues. Sanchez asks: "How can you ensure that the criminals will honour their commitment to delete the exfiltrated data? Is your organisation contravening legal or regulatory prohibitions against interacting with them?"

He adds: "The data you have paid to be destroyed is just as likely to turn up on the dark web, be shared among threat groups or even be accidentally released. The only sensible way to deal with these risks is to implement mitigations for them and try to prevent them from happening in the first place."

Mitigating these risks is not as difficult as it may appear at first sight. Businesses can materially decrease their exposure to cyber risk by taking a small number of key actions. For instance, implementing multi-factor authentication for all remote access to their systems is a simple and effective step that will greatly reduce the risk of having an incident. It is also important for organisations to understand that implementing these actions in a consistent and comprehensive manner are essential to their success.

The team at Beazley has seen examples in which MFA has been implemented, but those at the greatest risk of targeted phishing attacks – such as senior executives – have been excused from complying with that control. It is also not just a question of expediency or consistency; senior management and executives should also be leading by example to ensure that a culture of security is cultivated within the business. Also, a mismanaged cyber incident could turn into a D&O claim against the executives of a firm.

85%
of business leaders feel they are operating in a moderate to high risk environment

34%
of respondents rank cyber as their top tech risk now...

...but

44%
feel prepared to respond to it

19%
of companies cite employer risk as a major concern, up five points from last year

Beazley, 2022

A stitch in time saves more than nine

Some of these risk management measures will cost money and many will take time to implement. However, the fast-paced nature of technology innovation is also helping businesses. Where once a business would need to invest in new hardware and software – and the IT staff to manage it – new cloud services and solutions allow companies to implement and scale sophisticated risk management solutions that were previously only available to a large enterprise.

Executives must be seen to be monitoring cyber risk to strengthen business resilience. "We understand there's no silver bullet," says Sanchez. "Nor is there a magic money tree to cover every conceivable risk. But we can help clients identify which controls will have best effect and give them insight into cyber risk trends."

MacCabe adds: "We don't get paid for telling clients how to reduce their risks and improve their operational resilience. Our reward comes from clients with good risk management that protects their business and reduces both the corporate and personal risk so they don't become subject of a claim."

However, if the worst happens and a business does have to make a claim, then business leaders need to be sure that they have the right insurance partner who will help to successfully manage the claim on their behalf.

The more inclusive the discussion is between insurers, those responsible for risk management, the CFO, compliance, the responsible business team, human resources and beyond, the more comprehensive, coordinated and effective the risk planning, and therefore more valuable, it will be.

Visit the risk & resilience reports for further risk insight and analysis reports.beazley.com/2021/rr

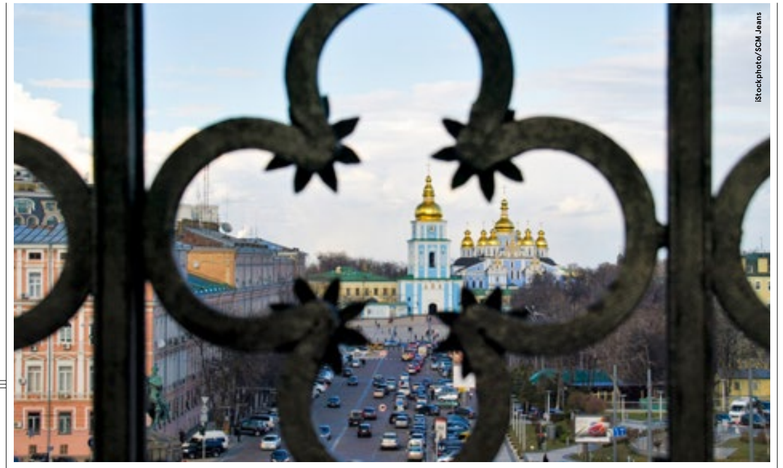
beazley

GEOPOLITICS

Digital sanctions have tangible effects

Digital sanctions represent a new frontier in global conflicts, with business-critical technology able to be switched off remotely. What impact will this have - in Russia and beyond?

Tamlin Magee



iStockphoto/SCM Jeans

Lenin once said there are decades where nothing happens and weeks where decades happen. This current period appears to be of the latter type. Just as the effects of the pandemic seemed to be on the wane, reignited geopolitical tensions in Europe exposed once again the vulnerability of global markets.

While the crisis in Ukraine has thrown supply chains into chaos, causing soaring wheat prices and sending petrol costs to an all-time high, the impact has been far-reaching in the digital space too.

Global technology providers have pulled their services from the Russian market in droves. Mastercard and Visa have restricted the use of Russian-issued cards outside the country, while Google Pay and Apple Pay are limited for customers of sanctioned banks, leading to queues in the Moscow subway as commuters are forced to pay with cash.

The plug has also been pulled on other digital asset. Some of these are self-imposed such as Russia's banning of Facebook and Twitter, while Netflix, Paypal, Adobe, Oracle, Amazon Web Services, Microsoft and SAP have all introduced their own restrictions on services in the country, making 'business as usual' almost impossible.

While these actions may be aimed at penalising the regime of Russia's president Vladimir Putin, they also affect consumers, startups and small businesses – the vast majority of which have nothing to do with the invasion and are also suffering the consequences. So notes Nigel Green, founder and CEO of financial services business deVere Group, which continues to operate in Russia.

"A few hundred, named Russian individuals are on the international sanctions list and, of course, we strictly adhere to it," Green says.

"But we are not going to roll out a blanket ban on ordinary, innocent Russian users. The situation is inevitably going to get worse, with potentially devastating consequences, as they are frozen out of the financial system."

This move to bring digital services into geopolitics has been slow but steady. In 2019, a raft of new sanctions against Venezuela meant that Adobe services were no longer accessible in the country. Microsoft's software sales in Russia were affected by previous US-led sanctions over the Crimea dispute, while developer platform GitHub was forced to block users in Syria, Crimea and Iran.

There is very little that businesses affected by these digital sanctions can do, other than await the outcome of a request for exemptions via the US Office of Foreign Assets Control, the authority in charge of overseeing sanctions compliance.

If that doesn't happen, there's piracy. Before Adobe was granted an exemption to operate in Venezuela in late 2019, designers in the country reluctantly turned to software theft because they had no other choice.

Russia is considering legislating for this approach by re-evaluating its copyright laws, as the Ministry of Economic Development proposes relaxing piracy rules to offset damage from digital sanctions.

Meanwhile Russians are turning to virtual private networks (VPN) to access digital services, says Corneliu Bjola, author of *Digital Diplomacy: Theory and Practice*. But this workaround may be short-lived. "The most popular VPN apps are based in France, the UK and the US, so in principle they could become part of the package of digital sanctions as well," he points out.

There are also rumours that Russia will cut itself off from the global internet, making a 'splinternet' – where countries choose to silo web access by national borders – seem closer than ever.

And this software flight may ripple into undesirable longer-term consequences for the West, such as a strengthening technological relationship between Russia and China, born from sheer necessity, and a recalibration of digital power.

"Chinese authorities are taking notes about how these sanctions are implemented and how it might be able to protect itself against something similar if the relationship with the US deteriorates in a similar fashion," Bjola says.

> **What can you do to help identify potentially emergent leaders? Because they're the people you're going to rely on in the aftermath**

He highlights that China's digital yuan could theoretically bypass SWIFT payments. "At the moment, the amount of international transitions seems to be low, but the matter could change rapidly if Russian companies discover ways to use it to evade sanctions."

That makes China a country to watch, since it is not clear whether its companies will comply with the US/EU/UK sanctions, says Bjola.

"The Biden administration has already signalled its determination to sanction Chinese companies if they aid Russia, so it will be interesting to see how China reacts to this. Purchasing Russian tech companies at a discount may prove tempting for some Chinese companies."

As moves are made on the geopolitical chessboard it is usually ordinary citizens who suffer. Of course, the immediate impact of displacement, death and regional instability has rightfully taken precedence in headlines during Russia's invasion of Ukraine. But organisations need to focus on resilience and business continuity plans.

Russia is facing digital sanctions after its invasion of Ukraine (pictured) last month

Although it is "hard to plan for such a devastating event", businesses should always have a disaster recovery plan in place, says Siobhan Aalders, vice-president of global communications for the freelance marketplace Fiverr.

As tensions increased in mid-January, Fiverr raced to secure the safety of its staff by evacuating its Kyiv employees – comprising 15% of the company's worldwide development team – to safer regions in Ukraine or outside the country.

Developers in Fiverr's Tel Aviv headquarters also backed up areas of the business the Kyiv team were focusing on. "As we developed a plan for our employees, we knew the R&D centre in Tel Aviv would be able to pick up any slack and execute on our roadmap," Aalders explains.

Meanwhile, as rumours persisted that Putin could take down communications and digital services in Ukraine, Fiverr's operations centre was standing up alternative means of communication for employees in the country just in case connectivity was compromised.

Shane Henry, CEO of disaster risk consultancy Reconnaissance Group, says it's vital that businesses plan for the worst kinds of risk, from natural disasters to man-made crises. That means conducting a "reality check" on the culture of an organisation, taking stock of its current standard of preparedness and being open to blunt feedback from internal and external stakeholders.

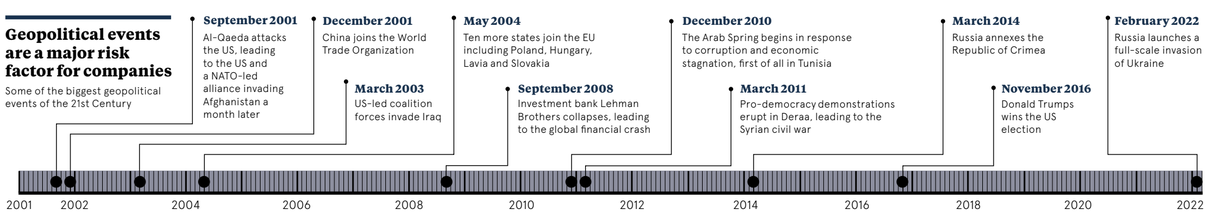
"How is it set up to calmly prepare for a crisis, whatever that crisis may be?" asks Henry. "And what is the impact on our people?

"A core component of that is to look at your leaders – not your executive team, but people that will probably emerge as leaders at all levels. We see that, between earthquakes, the aftermath of hurricanes and political fallout, companies have had people emerge as leaders at all levels.

"That raises the question: what can you do beforehand to help identify potentially emergent leaders? Because they're the people you're going to rely on in the aftermath." ●

Geopolitical events are a major risk factor for companies

Some of the biggest geopolitical events of the 21st Century



LEADERSHIP

Thinking the unthinkable

Information and agility are key for risk professionals, who need to look beyond current threats to predict the next major challenge

Virginia Matthews

It may be comforting for business leaders to look on the Covid pandemic and the invasion of Ukraine as once-in-a-generation events that could be neither anticipated nor planned for. Yet some would argue that far from being black swans, both the pandemic and the Russian invasion should have been high on the corporate radar, even if their precise impacts on business were less certain.

In order to better prepare for the next major threat, risk professionals must get a firmer handle on the information already available to them, says Oliver Harvey, global head of governance, risk and compliance at the intelligence software firm Nuix.

"One of the remarkable features of our age is that the world has never been more awash with data and, in theory, this provides a massive opportunity to reduce the number of 'out-of-the-blue' events," he says.

Yet he points out that many chief risk officers (CROs) are "overwhelmed by the sheer volume of intelligence" from many different sources. The UK's National Risk Register mentioned a global pandemic back in 2008 but few took heed. He believes that many businesses lack the skills necessary to interpret the relevance of such information to their own organisation.

Whatever their nature, all current and future risks to a business share a number of likely outcomes which should form the basis of the mitigation process, says Peter Groucutt, co-founder of IT disaster recovery consultancy Databarracks.

While many organisations, he says, base their risk and resilience assessment on theoretical 'what if' scenarios, he urges greater attention to the practical, on-the-ground impacts that risks tend to share.

"Regardless of whether it's warfare, malware, a climate change event or a nuclear disaster, your organisation could be locked out of its headquarters, face a serious loss of data, a cut-off of supplies and be vulnerable to a full-scale business collapse," he says.

While part of the job of being CRO is to "think about the unthinkable", as Groucutt puts it, many risk execs can become sidetracked by trying to predict both the nature of the next threat and its precise timing.

"While the potential impacts of a whole range of cataclysmic events are terrifying, they are easier to prepare for than the scenarios themselves. Many CROs seem to lack the insight to understand this," he says

> **In today's world, it all depends how far they're prepared to go and how much they're willing to pay to protect their business**

Whether the risk is an unexpected malware attack or a negative media report, picking up the signs of an impending event requires vigilance across a business.

"This is the perfect example of how diverse teams bring big business benefits," says Ahmed Badr, chief legal and risk officer at online payments platform GoCardless. "The more perspectives you have, the better you become at spotting what's coming down the line and anticipating risks that may seem 'out of the blue' to everyone else."

In the aftermath of the pandemic, risk and resilience have climbed up the boardroom agenda. While many firms have traditionally carried out risk assessments annually, should their frequency now be increased?

Yes, says Bolade Atitebi, senior vice-president of Mastercard Data & Services, who argues that the disruption caused by both Covid and now Ukraine should trigger a re-appraisal of risk and mitigation planning.

"Volatility, disruption and shocks will occur in the future, and maintaining an emphasis on emerging risks while not losing sight of risks already under the surface is the balance to strike," she says.

"Most organisations should have learned that the agility to assess business strategies on an ad hoc basis in order to address rising concerns is now critical. Preparation is key and likely to be more effective than prediction when it comes to out-of-the-blue risk."

Among the potential events that require specific mitigation are industrial action, terrorist attack, plane crash, flood, power, international conflict and future global pandemics, Atitebi adds.

While the impact of Covid caught many organisations by surprise, a global cyber attack – potentially as fall-out from the Ukraine conflict – could be equally devastating.

"A major attack on a public cloud provider could include the loss of data centres and suppliers, an inability to access your bank account and an office and team whose roles would be rendered fairly meaningless," Groucutt says.

EY, 2021

79%
of boards believe that improved risk management will be critical in enabling their organisation to protect and build value in the next five years

42%
of risk management leaders look more than five years into the future when scenario planning

83%
of board members believe market disruptions have become more impactful

28%
of risk management leaders look more than five years into the future when setting their organisation's business strategy

Do brands need a chief worry officer?

Facebook co-founder Mark Zuckerberg once famously presented a business card with the title 'chief worry officer' on it, while Coca-Cola boss James Quincey is said to use the same descriptor as a joke in internal meetings.

Post-Covid, the chief risk officer, someone who looks beyond a business's status quo to predict and mitigate against future risks, is an indispensable part of many C-suite line-ups. Yet being a professional worrier is only one of the qualifications needed to succeed.

A good CRO must also "understand psychology to prevent them from being adversely impacted by cognitive biases", says Oliver Harvey from Nuix. As well as this, they need a strong understanding of the business to effectively challenge internal norms, he adds.

The need to play devil's advocate is particularly suited to neurodiverse risk professionals, he argues, Often more adept than neurotypical colleagues at "seeing existing data in new ways", such CROs may also be able to "identify risks earlier and more dynamically".

While associating risk with worry could obscure the many and varied opportunities that come from challenging conditions, consultant Claire Trachet dislikes the 'worry' word altogether.

"I doubt a chief worry officer would be all that helpful to a company because while it's easy to find problems, what is often needed is the ability to take calculated risks – the definition of enterprise – and have a plan for when a crisis looms."

She believes that the best risk management "is done as a team". And she warns: "By always crying wolf, a chief worry officer would most likely end up not being listened to at all."

"The worst-case scenario for a commercial firm would be the loss of the entire business but, hopefully, there would be insurance to cover it. In the case of a hospital, say, the threat to patients would be at an entirely different level."

While such a major event may appear unlikely, routine malware attacks on businesses of all sizes have already become all too commonplace, he says. Yet many victims prefer to pay up rather than put comprehensive mitigation plans in place.

More than three-quarters of UK businesses were hit with ransomware demands in 2021, according to a report by data security company Proofpoint. As many as 82% paid the hackers to restore their data.

"Even when we do meet clients who are prepared to go the extra mile to keep their systems and data highly secure, we tell them that you can only plan so far," Groucutt says.

"We can back up their data, leave a copy of it on site, encrypt another copy and keep it safe in a cloud provider, copy it all to another cloud provider and even put it all on tape and bury it underground in a bomb-proof bunker lined with lead

"In today's world, it all depends how far they're prepared to go and how much they're willing to pay to protect their business." ●

> **The agility to assess business strategies to address rising concerns is now critical. Preparation is more effective than prediction**

Forget fires and floods – why disaster recovery should focus on ransomware

Dubbed 'the biggest online threat to people in the UK,' organisations should prioritise ransomware in their disaster planning, argues Zerto, a Hewlett Packard Enterprise company

Ransomware has been front page news in 2021. In a world of escalating cyberattacks, ransomware garnered attention with a series of attacks that targeted every type of organisation from utility providers to food suppliers to healthcare and local authorities. These services can struggle to recover months after an attack.

Such is the threat, the head of the National Cyber Security Centre (NCSC) described ransomware as "the biggest online threat to people in UK."

The problem is that some business decision makers still don't see ransomware in the same context as other disasters, like fires or flooding. Cybercrime is the only industry where the scale of innovation happens on the criminal side. The more they achieve 'success' the more we will see a rise in volume and severity, argues Andy Fernandez, senior manager, product marketing at Zerto, a leader in disaster recovery, backup and cloud mobility.

"At some point every organisation will be faced with a ransomware attack and will need to recover," he says. "If I was an organisation, my bigger concern is not 'will a natural disaster or outage happen?' It's 'I know I'm going to get hit by ransomware. How am I going to respond to that?'"

> **It's about finding solutions that can get you back up and running without paying the ransom**

Weeks of downtime post-attack

Many organisations with a disaster recovery and business continuity plan in place will be confident in their ability to recover following an attack. But one critical question remains: how long will it take them to recover their data, and how much damage will be done in the meantime?

"Often companies will be using legacy data protection," says Fernandez. "It's not just about: can I recover? It's about how quickly I can recover. By the time those organisations are able to recover their data – to become operational again – the business has suffered massive disruption. It can take days, even weeks, to recover data in those instances. We've seen organisations pay the ransom, even when they have backups available because they cannot afford to spend the time recovering from backups.

Importantly, data loss and downtime are separate things.

"There are two important metrics," says Fernandez. "The first is the recovery point objective (RPO), which refers to the potential data loss the organisation faces in the aftermath of an attack. When was the data last copied? Six hours ago, 12 hours, one day? The second is the recovery time objective (RTO), which is how short is the timeline from the point of encryption to the point of recovery?"

Continuous data protection

One answer is continuous data protection (CDP). CDP can reduce service levels — both RPO and RTO — from hours to minutes, even seconds. In fact, CDP recoveries can assist organisations in recovering to a state seconds before an attack, in just minutes.

While traditional methods of data protection take timed 'snapshots' as a way of backing up data, CDP solutions like Zerto continuously replicate that data. This can be to multiple sites, with no snapshots or performance impact with data being replicated every five seconds. This means customers can quickly restore entire sites and applications in minutes, at scale.

"It's about finding solutions that can get you back up and running without paying the ransom," says Fernandez.

'When,' not 'if'

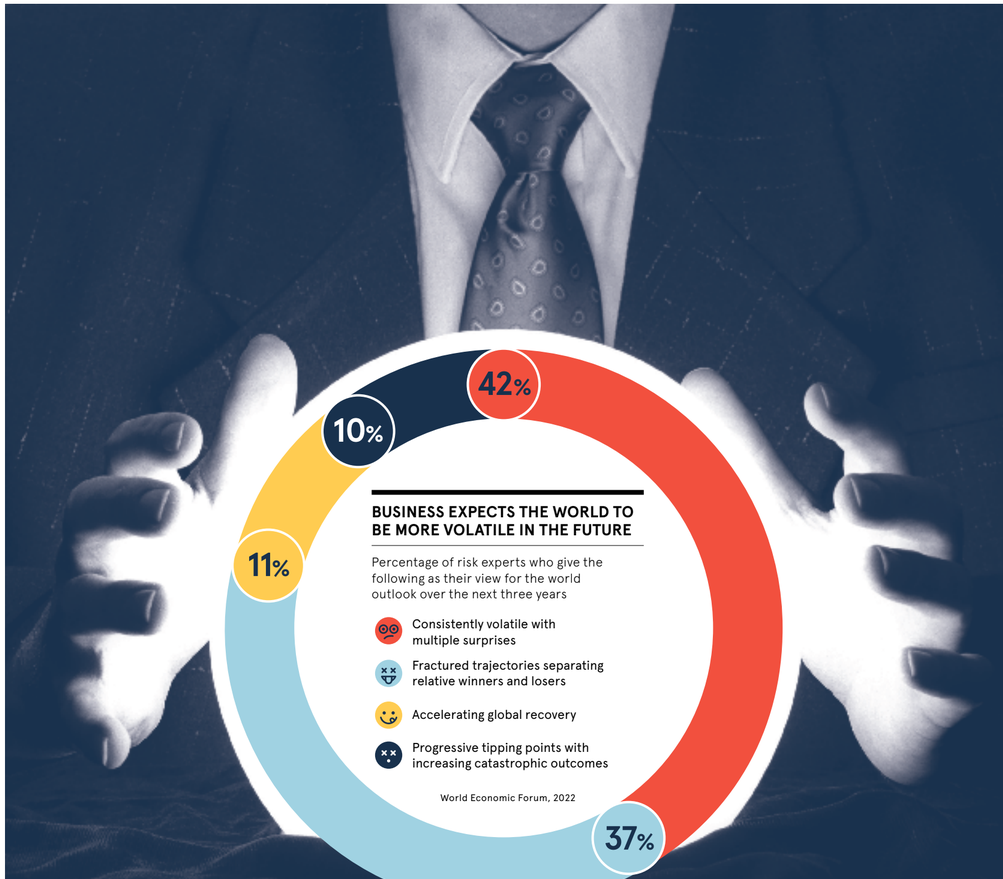
Research suggests it is a case of 'when,' not 'if' an organisation falls victim to a cyberattack. One IDC survey shows 95% of mid-sized and enterprise organisations have suffered a malicious attack – and more than a third have suffered more than 25 attacks.

Eight out of 10 of those attacks resulted in data corruption, with 43% of organisations experiencing unrecoverable data within the past 12 months.

"Whether you're the CEO or CIO, ransomware is not your IT manager's problem. It's your problem," says Fernandez. "Because it's a complete disruption that could tank your business – and will if you don't prepare correctly."

To find out more please visit zerto.com

Zerto
a Hewlett Packard Enterprise company



BUSINESS EXPECTS THE WORLD TO BE MORE VOLATILE IN THE FUTURE

Percentage of risk experts who give the following as their view for the world outlook over the next three years

- Consistently volatile with multiple surprises
- Fractured trajectories separating relative winners and losers
- Accelerating global recovery
- Progressive tipping points with increasing catastrophic outcomes

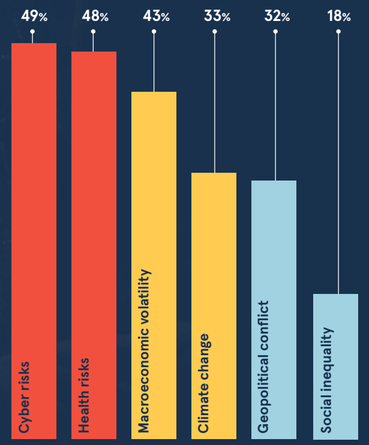
World Economic Forum, 2022

THE BUSINESS RISK OUTLOOK FOR 2022

2021 was a year of unprecedented disruption for businesses as cyberattacks, supply chain issues and climate catastrophes impacted companies' operations. Combined with the ongoing impact of the Covid pandemic and, more recently, war in Ukraine, business resilience is being tested like never before. But does the C-suite agree on the key risks and challenges for business – and therefore where they should focus attention?

CEOs ARE MOST CONCERNED ABOUT CYBER RISKS

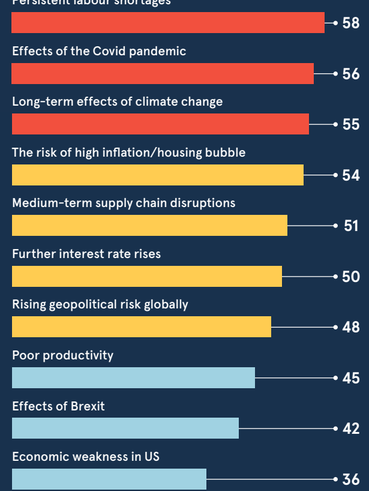
Percentage of CEOs who are 'very' or 'extremely' concerned about the following global threats negatively impacting their company in 2022



PwC, 2022

CFOs SEE LABOUR SHORTAGES AS THE BIGGEST RISK

Risks as cited by CFOs on a scale of 0 to 100 where 0 is no risk and 100 is high risk



Deloitte, 2022

Allianz Risk Barometer, 2022

FOR COOs, WORKER SHORTAGES AND EMPLOYEE TURNOVER IS THE BIGGEST CHALLENGE

Percentage of CMOs who ranked the following as the biggest headwind to growth in 2022

PwC, 2022

CMOs SEE TALENT ISSUES AS THE BIGGEST CHALLENGE IN 2022

Percentage of CMOs who ranked the following as the biggest headwind to growth in 2022

*may not add up to 100 due to rounding

Chief Outsiders, 2022

TALENT IS ALSO A BOARD-LEVEL CHALLENGE

Percentage of corporate board members who cite the following as important to their company's ability to grow in 2022

PwC, 2022

TECHNOLOGY

Code red: the growing threat from supply chain attacks

iStockphoto/ BalkansCat

Solarwinds was hit by a cyber attack that affected other businesses in its supply chain

With complex third-party cyber attacks exposing vulnerabilities in the digital supply chain, businesses need to be increasingly vigilant to protect both themselves and their customers

Alex Wright

Global supply chains have been exposed to unprecedented risk in recent years. A host of issues, ranging from Brexit and the Suez Canal blockage to the Covid-19 crisis and, most recently, the war in Ukraine, have all caused huge disruption.

But supply chain risk is not limited to the physical sphere. As businesses have grown exponentially thanks to increased digitalisation and reliance on third-party digital products, they have left themselves exposed to a growing cyber threat.

Supply chain attacks are when a company's data is compromised via the hacking of a third-party supplier with legitimate access to its customers' systems. Hackers can insert malicious code into trusted hardware or software at the source, compromising the data of its customers – and then their customers – in an onward chain.

One of the most devastating examples of this is the 2020 SolarWinds incident, referred to by Microsoft president Brad Smith as the "largest and most sophisticated attack ever".

In late 2019, the major US IT firm was targeted by hackers – later identified as originating in Russia – who used malicious code to gain access to the sensitive data of many of SolarWinds' clients, including technology giants Microsoft and Cisco, and the US Department of Homeland Security. In March 2020, SolarWinds began unwittingly sent out software updates to its customers that included the hacked code, which enabled the hackers to access their IT systems and data too.

The breach went undetected for months, with some victims not knowing whether they had been hacked at all. The full extent of the attack is yet to be determined, meaning it could take years to fully secure all the systems affected.

As companies have accelerated their digitalisation strategies to continue operating and to support their staff remotely during the pandemic, so they have become more dependent on third-party software and tech. This, in turn, has increased firms' attack surface exposure and points of vulnerability.

Supply chain attacks often start due to a mismanagement of critical access points. Known weaknesses in IT management platforms are then exploited, as evidenced by Log4Shell, a critical vulnerability in the logging tool Log4j that is used by millions of computers worldwide.

Hackers target victims through the key communication channels and software of third-party suppliers to gain access to their customers. A favoured attack method is through hijacked software updates – as in the SolarWinds case – which accounts for 60% of software supply chain attacks and disclosures, according to research by US think tank The Atlantic Council.

"Over the past few years, there has been an increase in next-generation supply chain attacks," says Ilkka Turunen, field chief technology officer at supply chain security firm Sonatype. "These direct attacks can involve, for example, malicious actors injecting new vulnerabilities into open source projects."

To combat the threat from these attacks, companies must have full visibility of all of their third-party relationships and dependencies. That means reducing the number of third-party providers they use, wherever possible, so there are fewer entities they have to monitor. Of course, this does not guarantee the integrity of their products.

"Regardless of the vendor's reputation, the product itself might have security gaps," says Heinrich Smit, who is deputy chief information security officer at cybersecurity specialists Semperis.

"When working with newer companies, be sure that you can view the company's product controls. Independent code reviews and application vulnerability reports are also very helpful because they evaluate a product inside the code and in situ from a penetrability perspective."

When assessing third-party suppliers, companies must ensure that they are thoroughly vetted and that their security practices meet the required standards. They also need to put in place a contract with the appropriate clauses to ensure they comply with the necessary regulatory and legislative privacy and security requirements.

Firms also need to analyse emerging third-party risks, as well as monitoring for suspicious activities on their systems and network. They should also only give network and systems access to those third-party vendors and apps that require it to perform their duties, and identify and monitor all access points.

Patching should be carried out on an ongoing basis, by ranking and scheduling updates in order of importance. In addition, organisations should regularly backup their systems to maintain their data.

This is in addition to having all necessary cybersecurity protocols in place and complying with the relevant data protection laws and regulations, as well as implementing ongoing staff training and knowledge updates.

Should the worst happen and a breach occur, companies must have a robust incident response and risk management strategy in place, as well as a disaster recovery and business interruption plan to ensure they get back on their feet with minimal disruption to services.

Organisations also need to understand and learn from previous cyber attacks, and shore up their vulnerable areas by carrying out internal penetration tests.

> **Over the past few years, there has been an increase in next-generation supply chain attacks**

One company that has considered these issues at length is E.ON. The European utility provider, which serves 53 million customers across 30 countries, recognised the need to expand its processes and procedures to protect itself and its customers from potential data loss via its third-party online ecosystem.

"To tackle the issue, E.ON first had to understand the risks it was exposed to," says Ran Nahmias, co-founder and chief business officer at Cyberpion, whose ecosystem security platform E.ON used to gain full visibility of its vulnerability to cyber attacks.

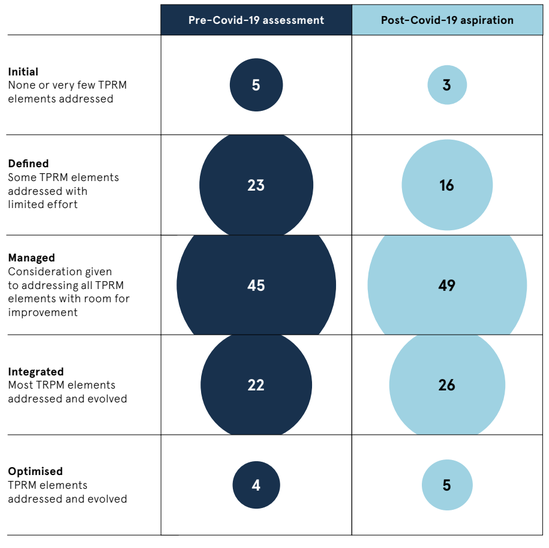
By carrying out an inventory of E.ON's internet-facing assets and the third-party assets it relies on, as well as the chains of vendor relationships, the company was able to understand its total risk exposure and allocate resources accordingly, reducing its exposure to operational disruptions and data loss.

While the complex threat from supply chain attacks remains, businesses that focus on analysing their exposure profile and mitigating the risks they discover give themselves the best chance of staying one step ahead of the hackers. ●

ORGANISATIONS ARE REALISING THE VALUE OF TAKING THIRD-PARTY RISK MANAGEMENT MORE SERIOUSLY

Deloitte, 2021

Percentage of organisations citing the following as their level of third-party risk management (TPRM) maturity



Commercial feature

Has your company reached 'data maturity'?

Data is crucial to decision-making, even more so when facing an unexpected challenge. Companies need to make sure they are serving the right data, to the right people, at the right time

Data is the foundation of any strong business. If you don't have insight into how your business is operating then you won't be able to manage – let alone see – the risks you're taking. Recent history has taught us the value of planning for the unexpected. Yet beyond global pandemics, there are new technical, legal and business challenges springing up all the time. As this happens, the companies that succeed are those which can best exploit the data they have to gain insights and make decisions about where to go next.

The issue often isn't a lack of data but that companies can end up with too much data spread across different systems that require different skills to access and analyse. Nearly four in five organisations make use of data from more than 100 different sources, with 30% making use of over 1,000, while nearly 80% store more than half of that data across multiple cloud services. The data usually exists, somewhere, but all too often cannot be accessed or analysed to give useful insights.

Organisations need more than just data, they need 'data maturity', which means serving the right data, to the right people, at the right time. The data needs to be high quality, highly relevant and compliant with regulations. The correct people need access to it – whether that's the CEO who needs high-level strategic insights or a marketing manager who wants to understand the performance of a specific campaign. And the time needs to be right: it's not good enough to understand what's already happened, you need to be able to see what's happening now and have a view of the future through tools such as predictive analytics.

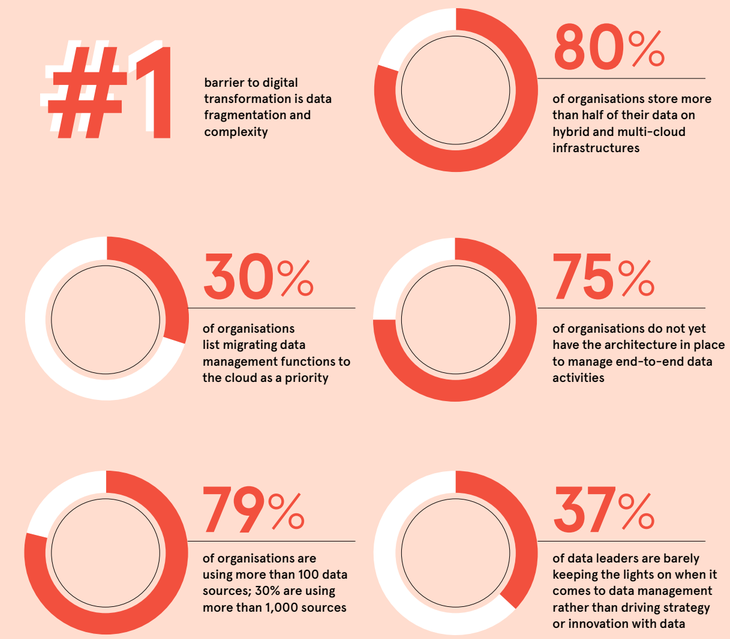
Yet with the business landscape constantly changing, even the data a company is managing can present risks as the important information they need to collect evolves. For instance, the amount of data relating to environmental, social and governance (ESG) issues that a business needs to understand is increasing. In the next few months, new regulations for firms operating in the UK will require reporting on the risks and opportunities presented by climate change, while those operating in the EU will need to abide by new rules requiring disclosure of the impact the firm has on climate change mitigation and adaptation.

Beyond regulation, firms are dealing with consumers who have a growing environmental, political, and social conscience about what they buy, how they buy and who they buy from. It's not enough to label a product as sustainable, businesses need to truly understand their entire supply chain to ensure every part of it actually lives up to the environmental and societal impacts they want to claim on the final product. Conversely, suppliers need to ensure they can deliver high-quality data about what they're supplying; companies themselves will increasingly make purchasing decisions based on the accountability of the supply chain they're hooking into.

One answer is to use a standardised data management platform that can deliver this level of maturity by ensuring the right level of data quality, compliance and access is available to help staff drive business decisions. This process doesn't necessarily require thousands of hours of manual work; increasingly machine learning and AI can be leveraged to ensure that the data is of high quality and that its presentation complies with GDPR and other governance rules, for example masking personal data where necessary.

IDC GLOBAL SURVEY OF THE OFFICE OF THE CHIEF DATA OFFICER

The study highlighted how critical data management is to digital transformation, noting that organisations with a high level of data maturity generate 250% more value from their data



Informatica

With this in place, firms can better understand the data they've gathered and turn it into actionable insight. As Greg Hanson of Informatica puts it: "Our intelligent data management cloud has helped organisations drive acquisition and retention with a more accurate view of a customer and their interactions with the business."

He points to the example of Verizon, who gained better insight into their customers journeys through having a cohesive data management platform. As a result they were able to deliver self-service digital resources that ultimately reduced call service volumes by 26 million a year.

> **Truly mature organisations will rethink data management implementations and make the strategic decisions that will allow them to identify risks, pivot quickly and drive value**

The pandemic saw organisations of all kinds pivoting to a digital-first approach and dealing with fast-changing levels of demand. Those that were able to implement, or were already implementing, intelligent data management experienced huge benefits. NYC Health + Hospitals, the operator of New York's public health system, was able to make use of intelligent data management to streamline its response. This covered everything from ensuring healthcare workers had better diagnostic tools to the rapid creation of dashboards to document and forecast the impacts on the service. The technology now in place can be reapplied to any future, large-scale health events.

In a different field, meal delivery firm HelloFresh was able to rapidly scale as it experienced increased demand as people opted to eat at home. This is because its robust analytics and forecasting systems meant that change in demand was immediately obvious to those who needed to see it, even with most employees working remotely. By definition, it is not possible to plan for unpredictable events, but when they happen, ensuring that high-quality data is immediately accessible to the right decision-makers means they can respond quickly and appropriately.

The pandemic and ESG regulations are just two examples of how the risks faced by businesses will continue to shift – both through sudden shocks and as legislation, technology and the consumer environment change. Businesses need to evolve to match changing risks. Those that succeed will be the companies that use data on past performance alongside real-time updates and predictive forecasting to make high-quality choices about how they operate.

Too often, data management as a discipline hasn't received the priority or focus it deserves, but if it's done intelligently it can actually push a business forward. Understanding the risks means understanding the opportunities. As Hanson puts it: "Digital maturity is a continuous process, not an endpoint. Truly mature organisations will rethink data management implementations and make the strategic decisions that will allow them to identify risks, pivot quickly and drive value."

For more information please visit informatica.com/platform

Informatica

SUSTAINABILITY

Firms cannot risk inaction on net zero

Many businesses feel overwhelmed by the challenge of cutting emissions, but doing nothing could be the most dangerous strategy of all

Bradley Gerrard

iStockphoto/Panya Kamthaisong

With humanity's impact on the warming of the planet now deemed unequivocal by the UN, the pressure is on every business to cut its carbon footprint. However, the problem can seem so overwhelming that it leads to the opposite result – no action at all.

It's a paradox. While customers increasingly pressure firms to blaze a sustainable, carbon-cutting trail, progress is too often confounded by a range of obstacles. These include fears over poor investment decisions, perceived concerns of a lack of knowledge, or worries about engaging someone without the genuine expertise demanded.

There will always be risks when change is necessary. But when it comes to climate change, it's rapidly become unviable to do nothing.

For many businesses, particularly smaller firms, it can sometimes seem that only transformational and radical change will make an impact. But think of it like running: if you're new to the exercise, it's best to stick with 5km jogs than attempting a marathon.

Nicolas Lefevre-Marton is a managing director of sustainability solutions at Engie Impact, which helps public and private organisations – including its sister energy firm Engie – to plan and implement sustainable strategies.

"Net zero is not a switch; there are milestones and steps," he says. "The most rewarding and easiest thing to do is to get a handle on the data and start to understand your emissions – where they come from and how they can change – rather than drowning in the concept."

Lefevre-Marton realises that even with the affordability of renewable energy falling and the likes of electric vehicles becoming cheaper, cost is one of the biggest risks for companies in achieving net zero.

"There's the economic risk, but there's also the regulatory risk. If you don't preempt these actions then it's possible you get caught out as the regulations can move faster [than expected], and if you're not ready to act, that's an issue," he says.

Preparedness therefore seems crucial. But even with improved knowledge and understanding, enacting change can be challenging.

"Mobilising organisations at the scale net zero demands has not been done before," he says.

With energy production representing close to 75% of global greenhouse gas emissions, it's intuitive that large energy firms, in particular, are prioritising the problem. But for smaller businesses and organisations, comprehending the issue and identifying the actions required can be a demanding task.

Mike Robinson is chief executive of the Royal Scottish Geographical Society (RSGS). It launched a Climate Solutions course two years ago to help distil the vast quantities of information available on climate change into manageable chunks and to help firms develop strategies and action plans.

"We're trying to reassure businesses that some things they can do are clear-cut," he says. "While some businesses might feel they want to wait, a lot of what we're trying to do is say that 'this is the direction of travel', so it's not about whether to do it, but when."

> **Net zero is not a switch; there are milestones and steps**

The RSGS believes there is a lot of opportunity in acting now, he says. "While there might be risks if you are a really early adopter of a new technology, there are plenty of things most organisations can do now to make a difference."

Robinson thinks many organisations that have taken steps to reduce their emissions seldom publish their efforts, believing their work will be criticised as insufficient. However, Climate Solutions has "accidentally created a safe space where people can ask daft questions and feel confident, which has been an important thing", he says.

Helping organisations to bridge the knowledge gap is one of the key aims of West Yorkshire's Manufacturing Task Force, established by Mayor Tracy Brabin, the former Labour MP for Batley and Spen.

Fiona Conor, managing director at Trust Electric Heating, is chair of the task force's net-zero group. It is working to help businesses understand how to measure and cut their emissions andidentify how to get funding to help implement changes, as well as trying to provide companies with comprehensive, but manageable, amounts of information.

Conor acknowledges that because small companies do not have the regulatory imperative to report their carbon reduction plans like their larger counterparts, progress could be slow.

But perhaps because of her marketing background, Conor sees publishing this information as an opportunity for firms to detail what they want to do, where they want to go and how they want to do it.

However, she acknowledges that "not all small businesses will believe there is a benefit unless there's lots of pressure to report it or demand from their customers".

There's another major issue for some firms, Conor realises: if they spend money improving the energy efficiency of their buildings, their business rates will rise, which can feel like they're being penalised for trying to do the right thing.

While a business rates relief for green improvements to buildings is set to be introduced in April 2023, many think the government can do more to encourage the transition to net zero, although this doesn't mean companies should entirely abdicate their responsibility to parliament.

First Wealth has a commitment to be net zero by 2030, which it introduced as part of plans to become B Corp-certified.

Anthony Villis is the firm's managing director. He says the company was initially weak in terms of understanding its environmental impact when securing B Corp status, but that measuring its carbon footprint in terms of scope one and scope two emissions was "fairly straightforward to get your head around". Scope one covers direct emissions, while scope two means the emissions that come from things such as electricity and heating bills.

More challenging are scope three emissions, which are those in the supply chain. First Wealth invests in roughly 10,000 companies through a range of funds and so quantifying that carbon footprint is almost impossible. But the quality of reporting around emissions is improving, meaning that wealth managers like Villis may soon be able to identify 'greener' funds via verifiable data.

While that will be a slow process, Villis is pleased with what his firm has already done and hopes that others will follow suit.

"We all have a role to play and everyone has a responsibility to do something, whether as a family or a company," he says. "It's about how businesses want to run: is it all about the bottom line and profit for shareholders or, like us, do you see an opportunity to grow a business that does good things too?"

For business owners and managers daunted by the prospect of tackling their carbon footprint, engaging employees should be the first step.

Villis says his firm has a shadow board with various subcommittees, including one focused on its environmental efforts. Robinson, meanwhile, suggests that the "single most important thing managers can do is to give permission for their people to make changes".

Lefevre-Marton adds: "Having a mission is hugely empowering for teams to work on, and there are few greater things that they can get hold of than decarbonising the world."

THE MOST SEVERE RISKS ON A GLOBAL SCALE OVER THE NEXT 10 YEARS

Chief risk officers rank the most severe risks

Economic · Environmental · Geopolitical · Societal

01	Climate action failure
02	Extreme weather
03	Biodiversity loss
04	Social cohesion erosion
05	Livelihood crises
06	Infectious diseases
07	Human environmental damage
08	Natural resource crises
09	Debt crises
10	Geoeconomic confrontation

World Economic Forum, 2021

INSIGHT

'Managing risk must be a dynamic and continuous process - and on every board's agenda'

Julia Graham, CEO of Airmic, and **Rachael Johnson**, head of risk management and corporate governance at ACCA , together examine how risk management must change and become more strategic as the world becomes more volatile

Q How are world events impacting how firms manage risk?

JG The pandemic, global warming and now events in Ukraine have forced organisations to rethink how they keep up with the speed of new risks emerging, the profile of known risks changing and how risk management practices need to adapt.

Gone are the days when a board reviewed its principal risks on an annual basis. Managing risk today must be a dynamic and continuous process - and on every board meeting agenda. It cannot be written up as part of an annual report then put away for the rest of the year.

Even in a great report, there's often still too much focus on the short term and the downside of risk, to the exclusion of thinking longer term and about the myriad opportunities well-managed risk can offer.

RJ Over the past few weeks, we have seen once again how the velocity and context of risk can change dramatically within a matter of days, if not hours, and how companies are affected no matter where they are based or what line of business they are in. Recent crises have forced organisations to rethink how they keep up with the speed of risk and they can only do that if they get their risk management framework - the principles, processes and the practices - better aligned.

We have seen even the most mature enterprise risk frameworks become disconnected from operational teams. Getting risk management into every conversation and decision across the organisation is key. It is the responsibility of the board to ensure that the risk management framework is fit for purpose, and properly resourced and aligned with the purpose and culture of the organisation.

Q How do companies better set themselves up to manage risk?

JG Space exploration, medical advances and new technologies all create seismic change and expand human frontiers, yet bring with them different and new risks. These are often hard to understand and difficult to insure, which means decision-makers must widen their field of vision to consider risks that could emerge or change as the world and business evolves.

As the frequency of global turbulence is increasing, managing risk is changing. Companies should use scenario analysis to understand the emergence and the consequences of risks. They can then use the outputs to inform ambiguities and identify any connectivity between risks, and as the basis for designing controls, including response plans and rehearsals for when things go wrong.

RJ Risk professionals have been candid about the questions they have to ask themselves and their teams. They need to stop looking at the past and instead offer more analysis about what is ahead - more foresight about what our expected and unexpected losses look like - if we are to remain relevant or have any success at steering organisations in the right direction.

Q How can risk professionals play a more strategic role in the future?

RJ In dealing with the risks we face, risk professionals have become multi-disciplinary and have had to work with others in a more continuous and coordinated way. Risk has never been so tied to performance, so it must be embedded in an organisation's strategy and, crucially, in the heart of its culture.

JG Risk professionals need to communicate effectively with the board and stand as trusted advisors. Companies that look longer term to build an organisation that is adaptable, agile and resilient will drive more sustainable growth. The modern risk professional has a leading part to play.

Julia Graham
CEO of Airmic (left)
Rachael Johnson
Head of risk management and corporate governance, ACCA (right)

Commercial feature

How centralising risk management can improve resilience

Operational resilience has traditionally been siloed across many teams, but a single vision can help companies mitigate against future risk

With the threat of cyber attack ever on the horizon, both the European Commission's 'Digital Operational Resilience Act' (Dora) and the Financial Conduct Authority's Operational Resilience regulations have been implemented to ensure all financial services companies adhere to a common set of standards around cybersecurity and operational resilience. The first major institutional framework for ensuring operational resilience, it is fundamentally changing the ways in which companies manage risk.

"You need to have a wider enterprise integrated risk management solution to cater for the requirement. Because what you generally find is that these solutions get built up in their siloes. With something like the Archer platform," says Chris Mann director for Archer European business, "you're able to achieve control harmonisation." With uniform regulation in place, companies can look across their business units and centralise risk and resilience strategies to ensure no gaps are left in the corporate defences.

But in the 10 years or so that operational resilience has become a key corporate need, ownership of it has sat within individual teams. Finance, say, looked after its own resilience strategy while digital did so as well. Now, the shift to centralisation is seeing organisation put the reins in the hands of a single leader within the company, says Mann. "It's starting to become the bridge to all of these different siloes," he adds.

That's been the case for global wealth management platform FNZ, which has built a culture of risk management that uses a strong framework for risk management that links to its operational resilience strategy.

It has deployed Archer's Operational Resilience tool, which enables teams across the organisation to operate within the same framework and standard for risk management. The system is configured to allow teams to use the same syntax across the company, while still enabling them to draw individualised, meaningful analysis from the data itself.

"Operational resilience is strong risk management and risk management done well," Kirsty McLaughlin, global risk systems manager at FNZ, says. "All we had to do was pull all those threads of data together."

Mann adds that ability to gain visibility across the organisation not only leads to a more resilient business, but a stronger reputation as well. "If you don't have the appropriate risk controls in place to sustain business longterm, you're going to have shareholder value issues and you're going to have reputational damage."

By aligning a company's many data sources and providing a more insightful analysis of that data will lead to "a single source of truth."

The two plus years of disruption the world has experienced has only elucidated further need for better insight and a stronger, more resilient business. Not only has Covid-19 affected business, but climate change has posed a risk to businesses around the world.

The Dora and FCA regulations are coming into force at an optimal time to encourage the financial sector to achieve operational resilience. "This regulation just takes that idea that you're never too big to fail and turns the dial a bit more," Mann says. He points to key aspects that could lead to an "operational downfall" – the likes of the ongoing climate crisis, supply chain disruption or cyber attack – as indicators that there's a greater need for organisations to prove to shareholders that they are mitigating risk wherever possible.

If companies can implement improved scenario analysis and risk quantification, as FNZ has done through the Archer Operational Resilience platform, they will be better placed to address future disruption. Similarly, quantification of risk, like with Archer Insight, can support decision-making with actionable information. Rachael Ward, head of group risk oversight – operational resilience at FNZ says, "Effective risk management enables our own management to safely deliver business strategy and plans...It maintains focus on the prevention of consumer harm, it supports risk-based decision-making, and also then delivers clear accountabilities across all of our lines of defence."

Defending a company in the financial services sector against disruption is of the utmost importance, affecting businesses and individuals around the world. With the new regulations in place, it is now the charge of companies to create operational resilience strategies that enable their businesses to come together behind a centralised framework and resource for understanding and mitigating risk.

For more, please visit archerIRM.com/operational-resilience

ARCHER

BRAND

Risking your reputation

Historically, there has been a poor understanding of the potential sources of reputational harm but risk management is moving up the executive agenda with new, proactive approaches

Michelle Perry


Unsplash/Zale Leray

Four days after Vladimir Putin's soldiers invaded Ukraine, the price comparison website Compare The Market pulled its TV ads featuring the animated Russian billionaire meerkat Aleksandr Orlov and his faithful sidekick Sergei from news bulletins.

The popular price comparison website's owner, BGL Group, said the fictional meerkat characters have no association with Russia and the current situation, and that it was continually reviewing its advertising.

The speed of the action would suggest a defensive move to distance the company from any association with Russia, as the world looked on aghast at Putin's attack

Reputational damage caused by any number of risks – accounting scandal, data breach or supply-chain issues – can ultimately destroy a company if management does not handle it well.

Historically, risk management – including reputational risk – has been overseen in a silo separate from executive leadership. In recent years, however, it looks as if executives are finally taking reputational risk seriously.

"They've pre-emptively decided not to put themselves in a situation where they can be reputationally damaged," Tricia Fox, of Cunningly Good Group, says of Compare The Market's move. "That makes sense. That implies that there are companies that take reputational risks very seriously and act upon it."

Compare The Market's decision is a modern-day example of how to tackle reputational risks before they become an issue. But few organisations have such a proactive communications division with a direct line to the boardroom. So, how should leaders act if faced with a damaging reputational event and how can they mitigate this risk?

Identifying potential issues and building a risk register are the first steps. Next, is devising a risk management strategy and ensuring all those responsible for this aspect of the business, including the communications department, are up to date.

The level of each risk will change depending on a range of internal and external factors, so the need to monitor the risk register and strategy regularly is critical. It must be a dynamic process.

"In general, there is a poor understanding of the sources of reputational risk and how to manage them. Situational awareness is everything. Monitor evolving threats and test their potential impact. Ask 'what if?' in relation to the current landscape, forward risks, historical issues and unforeseen events," says Ryan McSharry, head of crisis and litigation at PR firm Infinite Global.

Compliance is also vital. "The most effective way to mitigate reputational risks is to build a culture of compliance and resiliency. This means ensuring everyone knows what is expected of them by having a clearly articulated policy and procedure," says Lauren Kornutick, solutions manager for compliance at Fusion Risk Management.

Often, when an organisation comes up against a risk, it only becomes a reputational issue when it hasn't been handled swiftly, clearly and honestly. In today's world of social media and citizen journalism, the so-called 'golden hour' no longer exists. This means that, irrespective of whether the company's leaders know all the facts, it's critical that they publicly acknowledge the issue and explain how they plan to deal with it.

"Tell it first, tell it fast and tell it clearly. If you become aware of the issue and can head it off at the pass before the media gets wind of it, then do so. Take the initiative and, in doing so, you can control the message," says Paul MacKenzie-Cummins, founder and managing director of Clearly, a reputation management and PR agency.

If, however, the issue becomes public first, management can still recover control by acting quickly and honestly.

"In this instance, the advice is to acknowledge it and explain what steps are being taken to remedy the situation. Whatever you do, don't go into hibernation mode and hope it will go away – that will only fan the flames and exacerbate the damage to the organisation's reputation," MacKenzie-Cummins says.

Customers, employees and stakeholders are savvy. If they feel they have been deceived, the damage to reputation can spiral downwards very quickly.

Take the data breach at TalkTalk in 2015, when the company failed to publicly acknowledge the problem of hackers stealing thousands of customers' personal details, including bank accounts. At the time, the company faced a record fine and, ultimately, its CEO Dido Harding had to resign.

Recently, in the wake of a reputationally damaging incident, business leaders have tried shifting the negative public focus by adopting a new "favourable purpose" in its recovery. If this is a genuine, well-managed core strategy of change within the business, it can work. But often, companies choose this route of purpose for inauthentic reasons, which shrewd consumers and investors will quickly uncover.

"Consumers are an unforgiving bunch and will drop a brand or business in an instant if they feel misled. This is where responsible reporting is needed. Businesses need to hold themselves to account and demonstrate the tangible impact they are making, rather than paying lip service," MacKenzie-Cummins says.

In a fast-moving, interconnected world of global business, prevention is always better than cure. It's not uncommon for a company to lose as much as a third of its value because of a reputational risk.

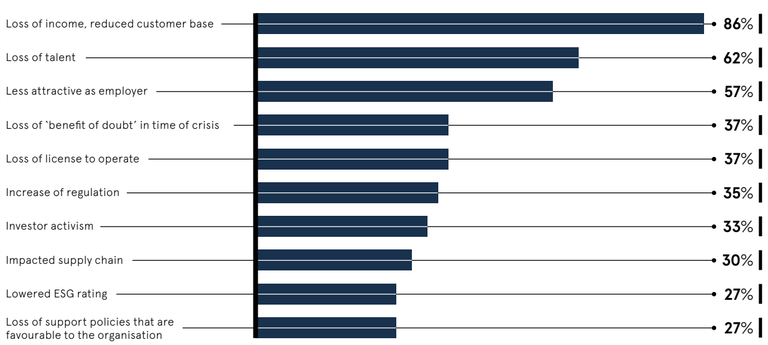
The investment a company makes in developing and managing a robust and well-monitored reputational risk management infrastructure is, ultimately, far less than the cost of responding to a crisis and the ensuing reputational fallout.

It's worth remembering that it takes years to build a good reputation but minutes to destroy it.

> Consumers are an unforgiving bunch and will drop a brand or business in an instant if they feel misled

COMPANIES FACE MAJOR LOSSES IF THEIR REPUTATION IS DAMAGED

Percentage of companies that cite the following as negative business outcomes that come as a result of reputation damage



Willis Towers Watson, 2021

SolarWinds and how it fixed a major reputational risk

In 2020, SolarWinds, a large US IT company with customers including the US Department of Homeland Security and the Treasury Department was hit by a sophisticated cyberattack that led to a data breach.

Sudhakar Ramakrishna, its CEO and president, took up the role just days before the data breach became public knowledge. Despite having the option of walking away, he instead took on the challenge of resolving the breach, fixing the damage to the company's reputation and building back lost trust.

Remarkably, just over a year into his role, he has achieved those goals. The company is almost back at its historical 90% customer retention rate, which had dropped to between 80% and 85% following the supply-chain attack. The firm has also recently begun acquiring new customers again.

Due to Ramakrishna's swift actions, the damage that the hack could have created ended up being far less severe than was feared.

Ramakrishna stabilised the company and fixed the breach by following a strict framework he devised. Called 'secure by design' it focused on three key things: what happened, how it happened and what we are doing about it.

Coupled with the framework, Ramakrishna enacted the strict operational principles of transparency, relentless communication, humility, belief in a solution and collaboration.

"Our focus was our customers and our business, while also dealing with the press, PRs, regulators and government. If the government wants to know something, collaborate with it, do not try to hide the issue and do not wish the problem goes away," Ramakrishna says.

He also spent months working with worried customers. "They have a right to be confused. They have a right to be angry. Don't brush it off, work towards engaging them," he suggests.

SolarWinds fixed the issues that allowed the original breach to occur, publicised the changes and communicated them to customers and the wider industry.

Today, the firm is, arguably, among the most secure in the world and one its customers trust again.

Realize the transformative power of data

At Informatica®, we create a world where data is poised for greatness, ready to deliver outcomes of unprecedented brilliance at a scale never imagined. With our **Intelligent Data Management Cloud**™, powered by CLAIRE, our AI engine, you can manage, govern, and unify all your data on a single platform. Transform your data from binary to the extraordinary.

Cloud First. Data Always.™

INFA
LISTED
NYSE

Trusted by:

84 of the Fortune 100

5,000+ active customers

cloud technology partners

Learn more at informatica.com

Informatica®
CLOUD FIRST. DATA ALWAYS.™