Control Risks

Global Resilience Survey 2020

Findings Report

Foreword

We can all agree that 2020 has been a turbulent year. It has provided a host of new challenges and opportunities for organisations across the globe and it has radically changed our risk landscape. Many organisations have acknowledged both the pros and cons of our adjusted reality and are actively updating their business strategy.

Crucially, businesses have seen that their long-standing practices of managing risk and responding to significant disruptions may no longer be sufficient to protect their personnel, assets, revenue, and reputation.

To better understand our clients' perspectives on these issues, Control Risks conducted the 2020 Global Resilience Survey and compiled the data to distil meaningful conclusions and trends to highlight how global business is practically implementing resilience programmes. This Report provides a fresh perspective on:

- How organisations are adapting and evolving their business resilience programmes after facing this year's challenges, including the COVID-19 (coronavirus) pandemic
- The differences in how resilience is understood and implemented in companies across all sectors and geographies
- How resilience fits into the broader organisational structure and can enable the business to succeed in a period of extended uncertainty

This Report provides you with unique analysis and recommendations from the Control Risks experts, as well as benchmarks and insights derived from more than 150 business leaders from 30 sectors across five continents.

Even though we all flexed our "crisis response" and "business resilience" muscles in dealing with COVID-19, this does not mean that businesses are ready for anything. Now is a time to reflect on what has worked well or fallen short and to use that knowledge to adapt our resilience strategies and to ensure that they are embedded across the organisations in which we work.

Join us in looking to the future and preparing for the global risks to come.

Nick Allan
Chief Executive Officer

Introduction

2020 has tested the limits and boundaries of organisational resilience like never before. Whilst some organisations have coped well with the impacts of COVID-19, others have struggled to adapt to an environment that requires flexibility, rapid decision making and clarity of communication. With uncertainty set to continue over the coming months and years, organisations have an opportunity to leverage their valuable skills and experiences to enable better strategic decision making and improved operational resilience.

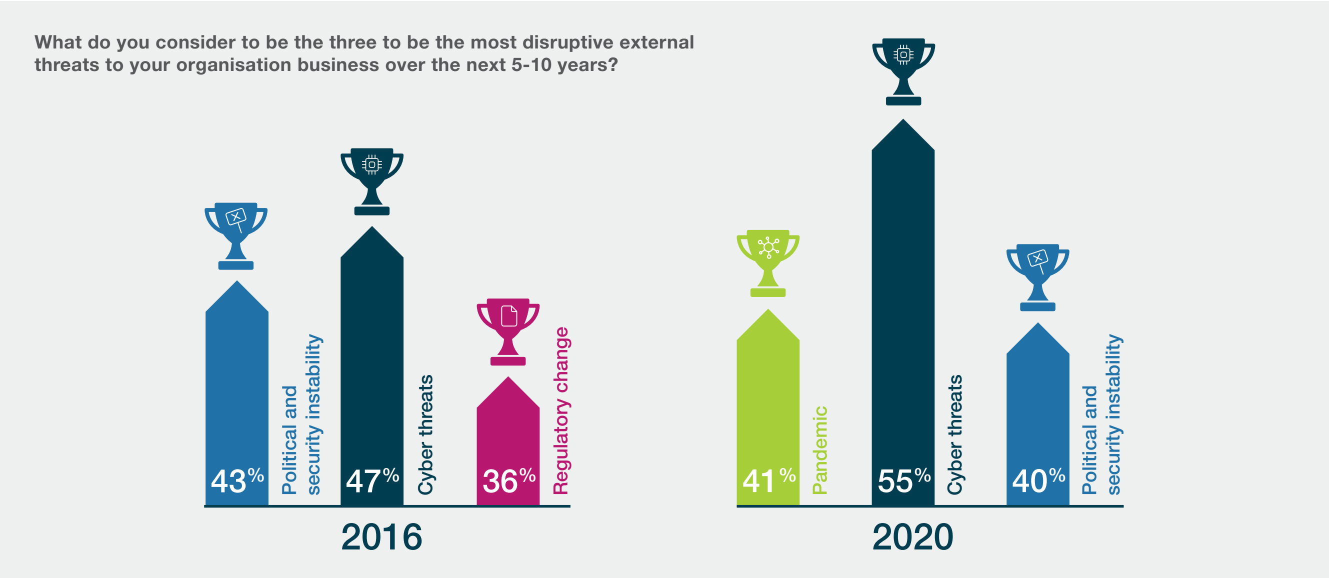
Against this backdrop, Control Risks launched the 2020 Global Resilience Survey to better understand how global business is practically implementing resilience programme especially after the onset of COVID-19 – and how companies are adapting the principles of resilience within their organisations.

In total more than 150 global business resilience leaders responded to the survey across all sectors and geographies, to provide insights into how resilience programmes have been implemented and perceived. Surprisingly, the findings were largely in line with the previous results from Control Risks 2016-17 Global Resilience Survey and 2018 report "The Evolution of Organisational Resilience", but with a few notable exceptions driven by responses to the COVID-19 pandemic.

This raised the question of whether companies were keeping pace with the changing threat landscape. But upon reflection, consistency over the past four years makes sense. Despite COVID-19, the **threat landscape hasn't drastically changed – rather, it has intensified**. The pandemic, in particular, has supercharged the scale and volume of cyber attacks we have seen over the last 11 months with targeting patterns mirroring the spread of the virus. While the tactics are not necessarily new, there has been a concerted effort to exploit fear and uncertainty.

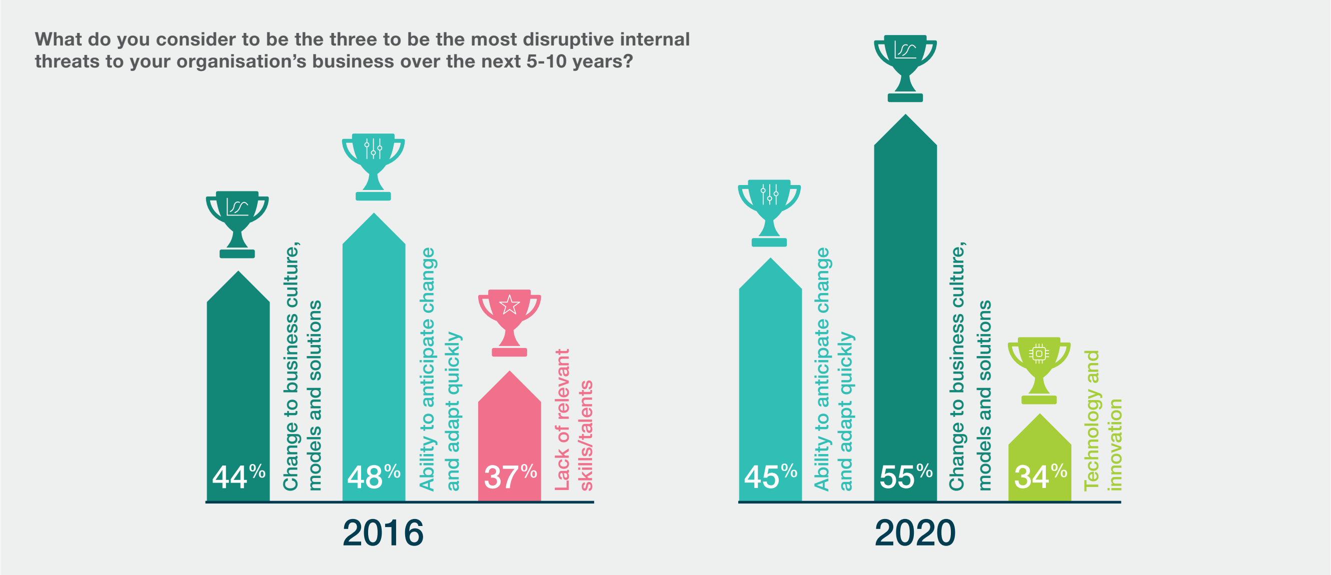
While we had (perhaps naively) assumed that organisations would have further strengthened their resilience programming and leveraged technology more effectively over the past four years, it is clear that the actions businesses need to take to become more resilient aren't too revolutionary, but are more important than ever.

Fig.1 ▸ Cyber threats remain a top concern for organisations



Source: Control Risks

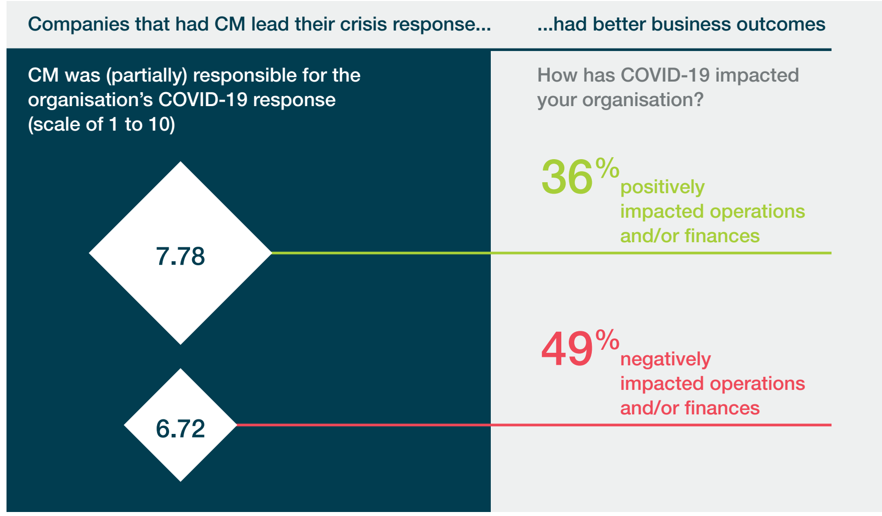
Fig.2 ▸ Change to business culture and the ability to adapt to that change remain the largest internal threats



Source: Control Risks

Interestingly, most survey respondents indicated that COVID-19 had a positive impact on how businesses deal with resilience. Across the board, Crisis Management (CM), Business Continuity Management (BCM) and Corporate Security received greater visibility and support this year due to their leadership during the COVID-19 response. Although the pandemic negatively impacted 49% of businesses, it also positively impacted 36% of businesses either operationally or financially. The **correlation between a mature resilience capability and positive business outcomes is no coincidence** – it indicates that companies that allow their resilience teams to lead operationally and strategically in a crisis, alongside senior leadership, reap tangible benefits.

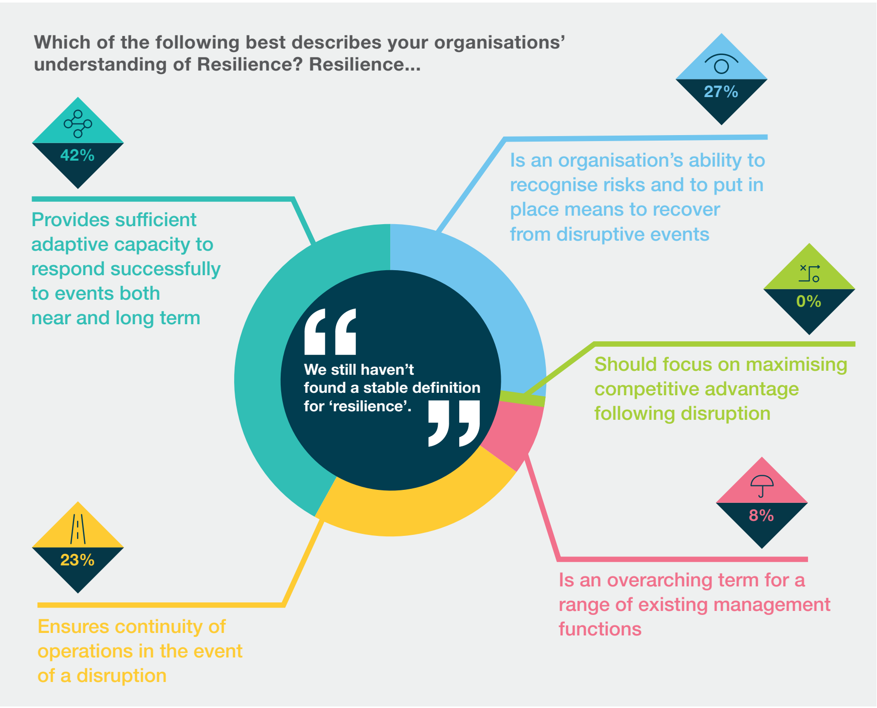
Fig.3 ▸ Positive business outcomes strongly linked to COVID-19 responses being (partially) led by the Crisis Management function



Source: Control Risks

The survey showed that "resilience" still does not have one common definition, nor is there consensus on how, or if, it should be used. 30% of respondents answered that their organisation does not use the term "resilience". Of those that do use the term, 65% of businesses describe resilience as "a proactive function detecting risk and disruption early" and use this information to make critical decisions followed by actions, 26% apply it as a "reactive function for responding to disruptions and incidents".

Fig.4 ▸ There is no unified understanding of what "resilience" is



Source: Control Risks

> "At Control Risks, our position is that a resilient organisation is one that understands its operating environment in the broadest sense, grasps the inherent risks and opportunities, appropriately manages its risks and, if things go wrong, are able to respond and adapt effectively to emerge stronger."
>
> **Jacqueline Day**
> Partner, Control Risks

The survey highlighted three key themes, which reflect on resilience practices and challenges the shape and scope of **resilience strategies** moving forward.

1. First, **most companies believe they have responded well to the COVID-19 pandemic, but that does not mean they should be complacent**. Now is the time to build upon successes and to maintain focus on mitigating the ongoing challenges of a new operating environment.
2. Second, resilience professionals **are playing a broader, more strategic role – and it's working.** The view that resilience professionals, such as CSO's are the operational protectors relegated to the back benches is antiquated and many companies are widening the scope and depth of their responsibility.
3. Finally, **a siloed approach to Enterprise Risk Management (ERM) is not enough to deal with today's rapidly shifting risk landscape**. Business functions that contribute to organisational resilience need to work seamlessly together with business operations to provide high quality risk intelligence and respond dynamically and effectively to both ongoing and emerging risks.

Most companies believe they have responded well to the COVID-19 pandemic, but that does not mean they should be complacent

Whilst most businesses acknowledge a challenging start to the crisis, 70% feel their ability to manage disruptions and adapt to change after dealing with COVID-19 has improved. For example, more than 90% of companies are confident in their ability to work away from the traditional office setting.

Much of that confidence is attributed to the all-hands-on-deck, "people first, business second" approach most companies took to the crisis. But a company's specific response is not the only factor that attributed to this perceived positivity – the global psyche and sense of unity in crisis also played a critical role.

The COVID-19 crisis is unique in many ways, one of them being that nearly every person and business globally was somehow impacted. The idea of "facing a common enemy" breeds goodwill that companies took as positive perception of their crisis response. Even amid record delays and lapses in service, consumers were lenient -- the blame lay on the pandemic or generic government restrictions, not on individual businesses. However, **it is not likely that the next crisis your organisation faces will impact the entire globe, so you should not expect that the same leniency and goodwill will be there next time.**

Whilst 93% of businesses were somehow financially impacted, only 5% of companies said their reputation was impacted or heavily impacted. A separate but related point: 78% of respondents identified reputational damage as a top general concern for their business compared to 58% for the risk of reduced revenue. This juxtaposition highlights the idea that financial impact is to be expected in a crisis whereas reputational damage is to be avoided at all costs; as long as that goal is met, companies can consider their crisis response a success.

Respondent testimonials

COVID-19 "tested our abilities… but we successfully achieved the new normal almost immediately"

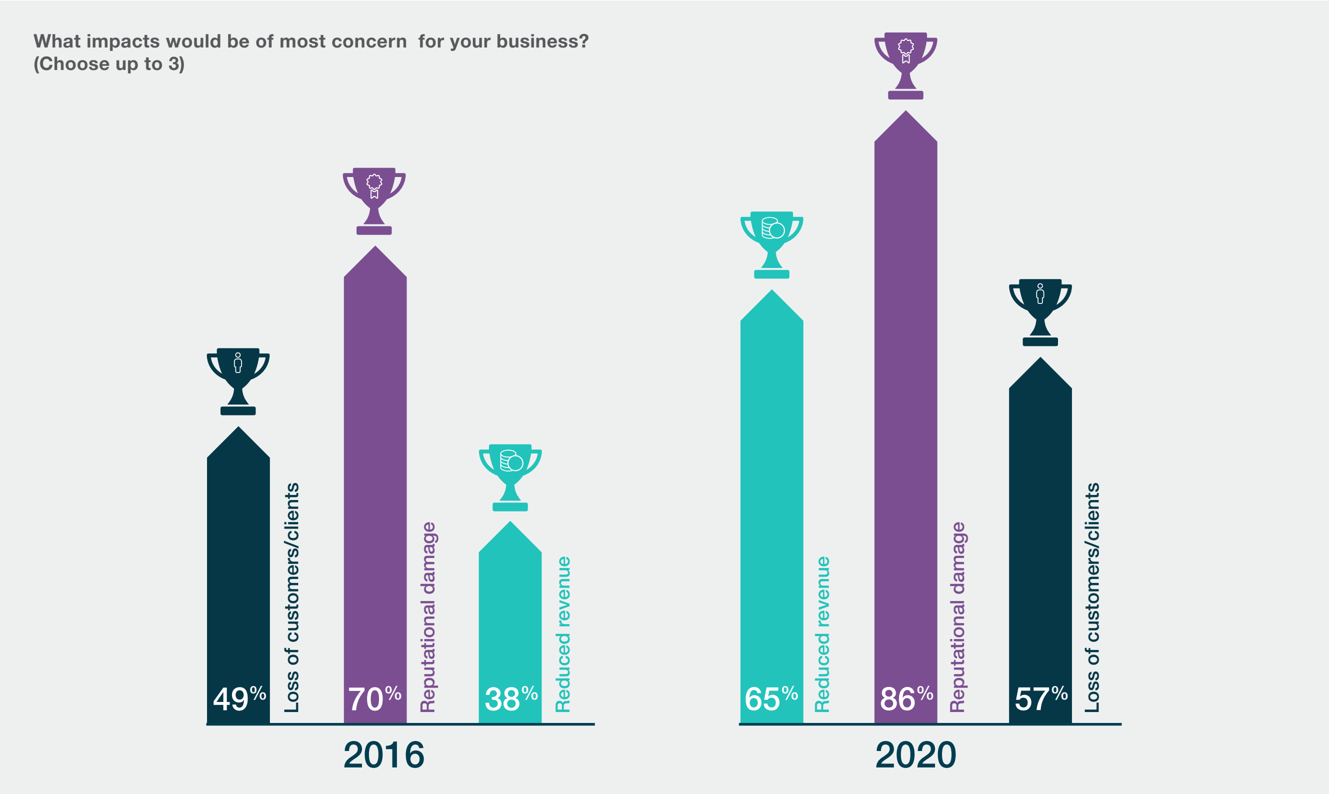
"The COVID-19 response program and our transparency have proven to be very effective"

"We came together as a team and solidified the importance of 'the team"

"You do not need to explain anymore why we have Crisis Management in our company".

Overall, there is a sense that "we didn't cripple as an organisation, therefore we succeeded." While COVID-19 may have lowered the bar on the definition of success, we would caution against this line of thinking. Complacency runs counter to the mindset of continuous improvement that truly resilience businesses must embrace and maintain.

Fig.5 ▸ Reputational damage is still a bigger concern than reduced revenue, even in today's economy



Source: Control Risks

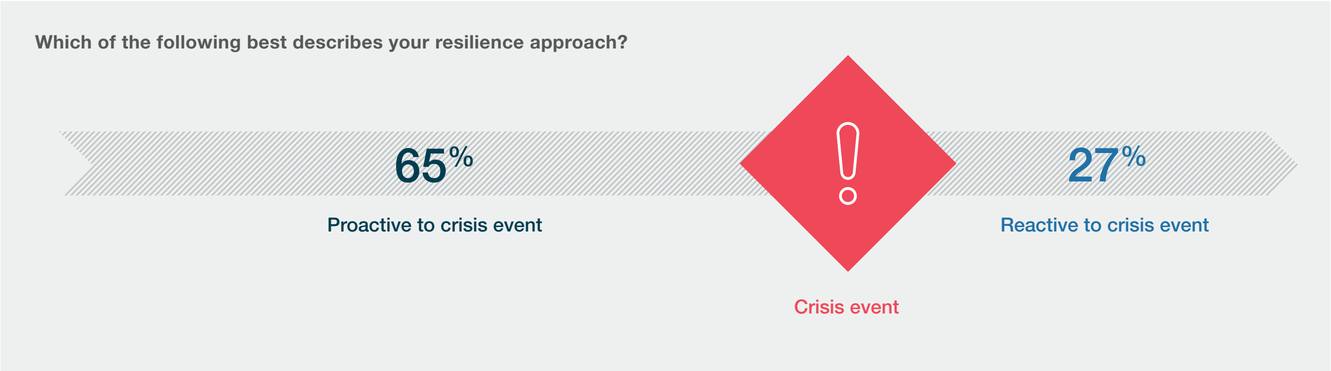
Resilience professionals are playing a broader, more strategic role – and it is working

Resilience is agnostic in nature, and therefore can be interpreted differently depending on a business' culture, organisational maturity, risk tolerance and profile. When identifying the functions that most contribute to their organisation's resilience programme, respondents clearly stated that BCM (52%), Risk Management (43%) and CM (41%) were the top three. In 73% of companies, Corporate Security owns or is heavily involved in their company's resilience strategy. In some regions such as Europe, resilience professionals have enjoyed a broadening scope of responsibility and increasingly strategic positions over the past two decades[1]. In others such as the United States, these professionals have traditionally maintained a more siloed or operational role. But there is one globally-applicable fact: **COVID-19 has reinforced and augmented the trend of resilience-related business functions collaborating and assembling under one leader**.

For some, COVID-19 "brought the Corporate Security team to the forefront" for the first time. For others, the pandemic "bolstered the role of the Crisis Management function in providing strategic decision-making and guidance in handing the impact of the event … from both macro and micro perspectives". More mature Fortune 500 respondents noted that COVID-19 "reinforced Corporate Security's effectiveness and value" and what was "already a well-recognised system/practice, now [had a] raised in profile across the company." Regardless of the company's size – from a family business to the Fortune 500 – having strong and strategic corporate resilience functions are key to being resilient and adaptable to the ever-changing business environment.

Whilst Chief Security Officers (CSO) historically have been a part of the crisis management teams, in many cases during COVID-19, they went from active participant to facilitator or leader almost overnight. Working closely with Human Resources, Legal and Communications, they played an instrumental role in successful responses to COVID-19 given their deep understanding of both people and facilities, two of the most impacted areas over the last 11+ months. This impact has been felt from the board room to the factory floor and we're slowly seeing the remit of the CSO evolve as Boards, CEOs and other senior leaders have increasingly recognized the immense value they can bring when dealing with delicate people-related crises.

Fig.6 ▸ Two thirds of respondents apply resilience as a proactive function



Source: Control Risks

[1] See Demos' 2006 "The Business of Resilience – Corporate Security for the 21st Century" and Control Risks' 2018 "Evolution of Organisational Resilience" report

The majority of companies that had formally coordinated the resilience functions prior to COVID-19 reported fewer operational disruptions and financial impact from the crisis. According to the survey, before COVID-19, 62% of CSOs "owned" Crisis Management (CM), whilst 20% "owned" Business Continuity Management (BCM). After nearly a year of dealing with the pandemic, these percentages are growing as businesses are further expanding the departments and types of risks overseen by one lead entity, often Corporate Security. This allows them to better fulfil their duty to protect their most critical assets including their people, facilities, intellectual property, and reputation. As demonstrated by the survey, ever more companies are realising that **integrating the management and strategy of resilience functions (in some cases, including IT security) makes business sense**.

By harnessing this momentum, resilience professionals can further secure their seats at the leadership table and showcase their strategic and operational insight and deep expertise in both CM and BCM. So where to from here?

Here are four ideas:

01

Resilience professionals should maintain and grow their posture within the organisation, even after COVID-19 is controlled. Most of the major people-related threats, risks, and crises that companies face, and will continue to face over time, could benefit from a resilience expertise and leadership. Future pandemics, violent protests, workplace violence, IP theft, terrorism, kidnap, extortive crimes, and other insider threats – these threats must be taken seriously and resilience professionals should be provided with enough resources and funding to put reasonable preventative and monitoring-based measures in place to adequately manage these risks. Simply ignoring them, as many did with pandemics in the past, could mean serious impacts to the organisation.

02

Involve the CSO in cyber security and incident management. We are increasingly seeing a convergence of cyber and physical security functions, as organisations recognise that incidents these days are not simply black and white, and often pose both digital and in-person threats. Threat actors are rapidly evolving their techniques to move beyond enterprise IT systems. Most organisations are still in the awareness phase, but with attack vectors expanding, security and risk management leaders need to update and unify their current threat management strategies to factor this all in.

03

Involve the resilience teams in ongoing ERM efforts. Historically, "people safety" appears as a vague and ambiguous risk on a company's risk register, but COVID-19 is showing that people safety needs to be examined in both a more holistic and detailed way. Getting the resilience teams involved early and often as a key leader and influencer in identifying, assessing and managing the organisation's top risks will benefit the organisation from Day 1 and likely result in a safer work environment for all employees, vendors and customers. Resilience professionals also will bring in a practical, more "boots on the ground" perspective that many board-led, compliance-focused ERM efforts are missing.

04

Formally align crisis management and business continuity capabilities. Resilience leaders demonstrated that during COVID-19 bringing together these two often-segregated response capabilities and fusing them will provide for a more effective and seamless response, but also provide potential efficiencies in the day-to-day management and resourcing of the capabilities.

COVID-19 has shone a light on the often underappreciated yet incredibly valuable role of resilience professionals. Companies are now at a crossroads and can take better advantage of their experience and expertise to capitalize on people-based opportunities. As more people return to the office, employees and customers will expect to be walking into a safe and secure environment, meaning there is even more pressure to 'get security right' in the near future. By elevating the role of resilience leaders and recognizing the value that they bring through increased, proactive resourcing, organisations will feel increased comfort that they are meeting their Duty of Care requirements, in perhaps a more efficient and effective manner than has been so in the past.

A siloed approach to Enterprise Risk Management (ERM) is not enough to deal with today's – and tomorrow's – rapidly shifting risk landscape

While some sectors, such as Financial Services, have vigorously implemented ERM and found it to be effective from a governance and compliance perspective, others have struggled to robustly build and/or run strong ERM programmes. For all, the practices of using audits to identify, measure and prioritise risks, and define specific mitigation strategies mostly work with short-term, traditional risks.

COVID-19 – which is clearly not a short-term nor a traditional risk – significantly challenged organisations' ERM programmes. Some survey participants noted that their existing ERM model wasn't suited to deal with the fast changing, often operational risks, posed by the crisis. This underlines the emerging reality that **dynamic, broad and fast-moving risks need a fresh approach that is aligned with resilience and supported by robust risk intelligence**. We believe that companies that adopt a fluid and risk-agnostic approach to risk management are more resilient and can better manage long-term, evolving crises.

Companies who currently employ ERM do not need to reinvent the wheel – they can overlay a resilience methodology to create a more holistic approach, which includes non-traditional, high-impact low-probability risks. This allows organisations to become capable of thinking beyond BCM and CM, beyond traditional risks like terrorism or natural disasters, and move to the strategic level of planning for scenarios like public policy and perception changes or expanding definitions of duty of care.

How can companies grow beyond traditional ERM and truly become resilient?

- Companies can think beyond standard risk management by using a resilience model which includes horizon scanning, scenario planning, and emerging risk identification. The model needs to include robust risk intelligence which ingests information from a number of external sources ranging from the strategic, such as geopolitics and supply chain, down to the operational, such as local security risks and local infection rates.

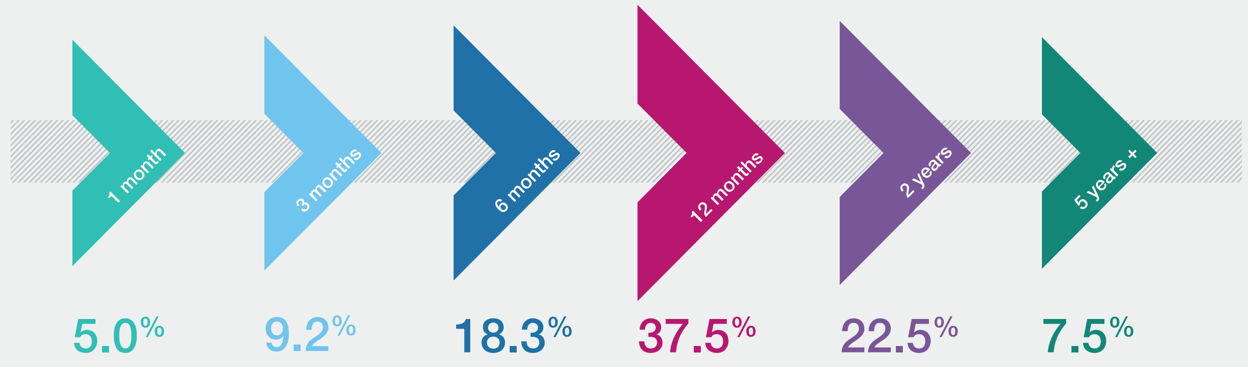
  Key risk indicators can be used to flag key information for risk and resilience professionals. For example, several large technology and manufacturing firms are now using a joint risk and resilience approach to actively monitor the risks to their strategic supply chain. Once key indicators are triggered, risk and resilience teams work seamlessly together to communicate and mitigate the risks, in this case moving strategic sourcing to other low COVID-19 locations.

- Consider bringing together business functions and expanding interdependencies to further embed resilience, and proactively scan the horizon for risks, changes, and disruptions. Resilient companies **conduct forward-looking scenario planning sessions that include event triggers to define when a scenario becomes more (or less) likely**, which is critical as it allows leadership teams to think through broad, inter-related risks and define concrete triggers that would then prompt business decisions.

- It is also essential to establish key performance indicators (KPIs) to measure success and determine their level of resilience maturity. 39% of respondents have established KPIs to benchmark their resilience. This practice greatly differs geographically, as well as by sector. While 46% of North American respondents use KPIs, only 27% of their European counterparts do the same. 54% of businesses in Financial Services reported they used KPIs, compared to literally none of the Oil and Gas respondents.

Fig.7 ▸ Two thirds of businesses monitor and analyse risks 12 or more months in advance

How far ahead of time does your organisation monitor and analyse risks?



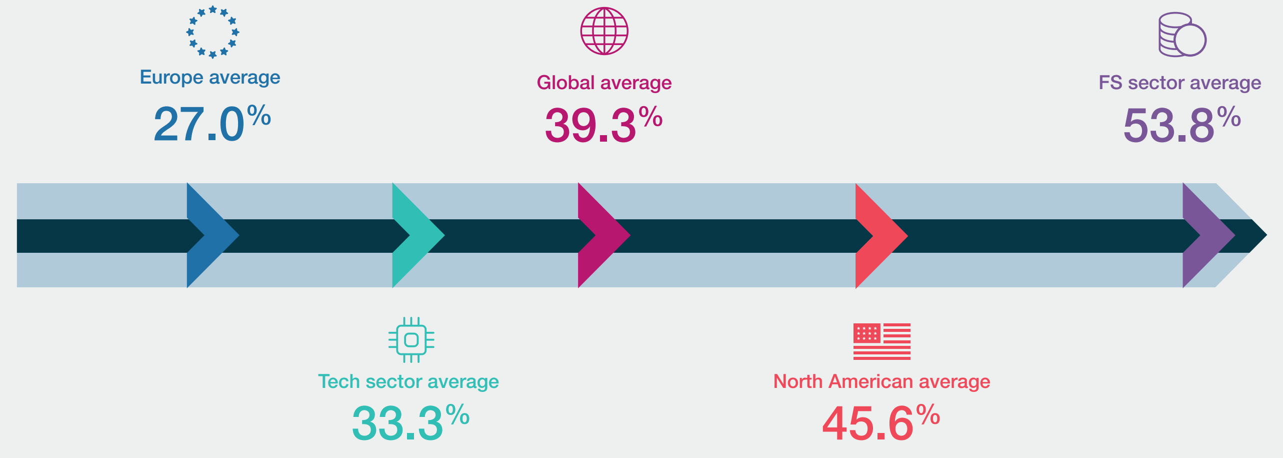
Source: Control Risks

Companies that have truly, fully implemented resilience throughout their organisation are very rare. They have spent significant time and effort into embedding their resiliency and deal with uncertainty and change centrally, with clear intent and coherence, and leveraging their corporate values and culture to embed the principals of resiliency.

Keep in mind that **a business' level of resilience maturity fluctuates** – it's not that an organisation which has checked all the above boxes can consider the job done. No one organisation can maintain a high degree of resilience all the time - crisis, disruption and change is the great equalizer. These factors will shift a business up and down the resilience continuum, the trick is to find the balance against a company's specific risk profile and risk tolerance.

Fig.8 ▸ Use of KPIs varies significantly by geography and sector

Has your organisation established KPIs and/or a set of metrics used to audit, monitor and evaluate your organisation's resilience performance or level of maturity?



Source: Control Risks

> "Aligning risk with a resilience methodology gives a company the flexibility and elasticity to proactively deal with protracted, complex and evolving crises."
>
> **Mark Whyte**
> Partner, Control Risks

Now is the time to actively build your resilience capabilities

Now sit back and think: where does your business lie on the resiliency continuum? How can you build upon the momentum from your success to further strengthen business resiliency? A strong resilience strategy gives organisations the ability to detect, identify, and respond to risks – giving them the confidence to take informed risks, capitalize on opportunities, and gain a competitive advantage.

So how do you get there?

First, look back. Bring your resilience functions and teams together and take an honest, deep look back at your corporate COVID-19 response. How did your corporate level respond and was the support provided to subsidiaries useful? How did your key country programmes deal with the crisis? How was the intra-company coordination and coordination with external stakeholders? What workarounds and new systems did you put into place that you want to keep and are they fully compliant?

Second, set short- and mid-term action plans to build your resilience capabilities. It's not just a question of adding resources to a resilience programme -- only 28% of businesses believe that increasing their resilience budget would strengthen their ability to withstand major disruptive events. Instead, it's a question of strengthening employee knowledge of crisis management practices (48%), strengthening internal communication (35%) and getting more executive teams and Boards to buy-in (31%) to raising the status and impact of corporate security and CM departments.

We highlight the importance of gaining executive buy-in now, after a massive crisis has hit and the clear and continued value of strong CM, BCM, and Corporate Security programmes are fresh in everyone's minds. Now is also the time to ensure that your data backup and retention capabilities are up to date, given the increase in ransomware and other cyber attacks.

Finally, practice makes perfect. **If there was one major lesson from COVID-19, it was that we learn best by doing**. At this point, most companies have well-seasoned, cross-functional leadership and crisis management teams. Continue to build their capability through simulating complex crisis scenarios that incorporate left-field incidents, risks, and/or threats. Don't only focus on more frequent incidents such as a ransomware attack or a building fire, but use the recently expanded response capabilities to stretch into more complicated scenarios such as an increase in public activism targeting your company, or an insider risk combining human and cyber threat vectors. Then, incorporate the lessons learned through these practice sessions (as well as any real-life incidents you or your peers may experience) to further strengthen your capabilities.

If you would like to find out more about the Global Resilience Survey and analysis, or talk to our experts about practical ways on how to strengthen your company's resilience strategy, please reach out to

Caroline Naumann
Associate Director, Frankfurt, Germany
caroline.naumann@controlrisks.com

Matt Hinton
Partner, New York, USA
matt.hinton@controlrisks.com

Mark Shortman
Principal, Sydney, Australia
mark.shortman@controlrisks.com

Mark Whyte
Partner, London, UK
mark.whyte@controlrisks.com

Andy Cox
Partner, London, UK
andy.cox@controlrisks.com

Jackie Day
Partner, Washington DC, USA
jacqueline.day@controlrisks.com