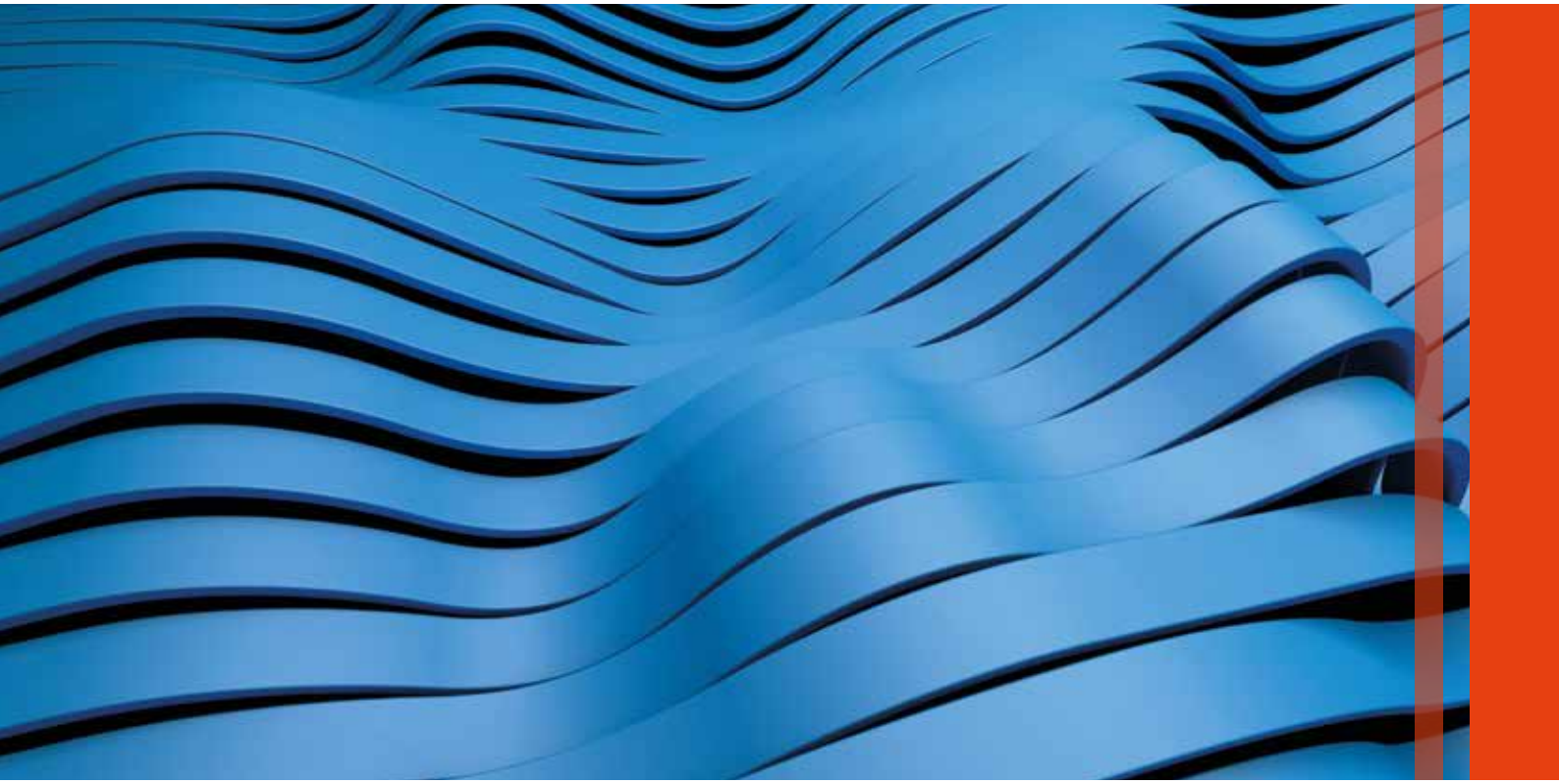
Control Risks



THE STATE OF ENTERPRISE RESILIENCE

SURVEY 2016/17

This survey is supported by

airmic

Managing Risk | Maximising Opportunity

Control Risks is a global risk consultancy. We help some of the most influential organisations in the world to understand and manage the risks and opportunities of operating around the world, particularly in complex and hostile markets. Our unique combination of services, our geographical reach and the trust our clients place in us ensure we can help them to effectively solve their problems and realise new opportunities in a dynamic and volatile world. Working across five continents and with 36 offices worldwide, we provide a broad range of services to help our clients to be successful.

Published by Control Risks Group Limited ("the Company"), Cottons Centre, Cottons Lane, London SE1 2QG. The Company endeavours to ensure the accuracy of all information supplied. Advice and opinions given represent the best judgement of the Company, but subject to Section 2 (1) Unfair Contract Terms Act 1977, the Company shall in no case be liable for any claims, or special, incidental or consequential damages, whether caused by the Company's negligence (or that of any member of its staff) or in any other way. ©: Control Risks Group Limited 2016. All rights reserved. Reproduction in whole or in part prohibited without the prior consent of the Company.

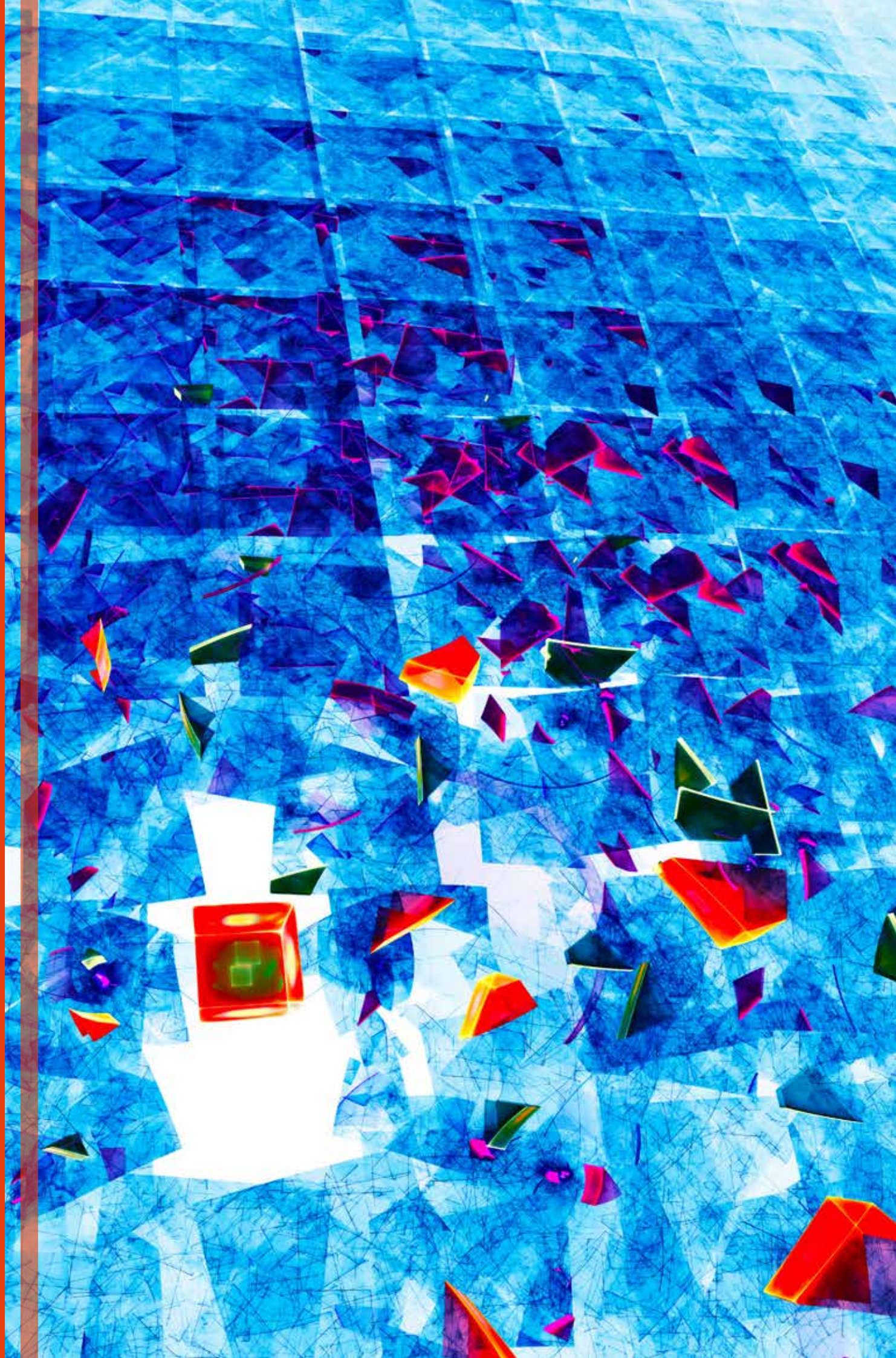
TABLE OF CONTENTS

FOREWORD

In August 2015 Control Risks conducted a global resilience survey across its client base and wider contacts to gain a better understanding of the degree to which the concept of resilience has gained currency and has become embedded within organisations. We sought to address issues such as how companies monitor and analyse the risk landscape, organisational risk governance, and the gap between theoretical understanding and practical application.

In Control Risks' 2016/17 global resilience survey we focused on the practical implementation of resilience, and how businesses are striving to adopt some of the principles of resilience in their organisations.

There continue to be a wide range of views on what resilience means, its component parts, and the tangible benefits that may flow. However, Control Risks increasingly sees a growing impetus to move on from definitions to building resilience. It is apparent that between resilience enablers such as business continuity, risk, and technology professionals and the board, there seems to be a slightly different understanding of what resilience means at a corporate level. However, with the imminent publication of ISO 22316 'Security and Resilience – Guidelines for Organisational Resilience' the debate has now progressed from one concerned with definitions and concepts to one of implementation and the realisation of the benefits of a comprehensive and integrated approach to embedding organisational resilience.



INTRODUCTION

The draft of the ISO 22316 articulates resilience as having a dual role. It is about an organisation being able to identify, analyse, and implement planning to be better able to recover or 'bounce back' from disruptive events, but it is also about the organisation's ability to adapt to change in both the short and longer term.

Regardless of whether one agrees with the definition outlined by ISO, or has a slightly different perspective, the principles of resilience are becoming common parlance. Control Risks' survey seems to support the view that organisational resilience ultimately requires a collaborative effort between many management disciplines. Only if collaboration between management disciplines is achieved, together with the ability to identify and successfully manage risk, can an organisation become truly resilient.

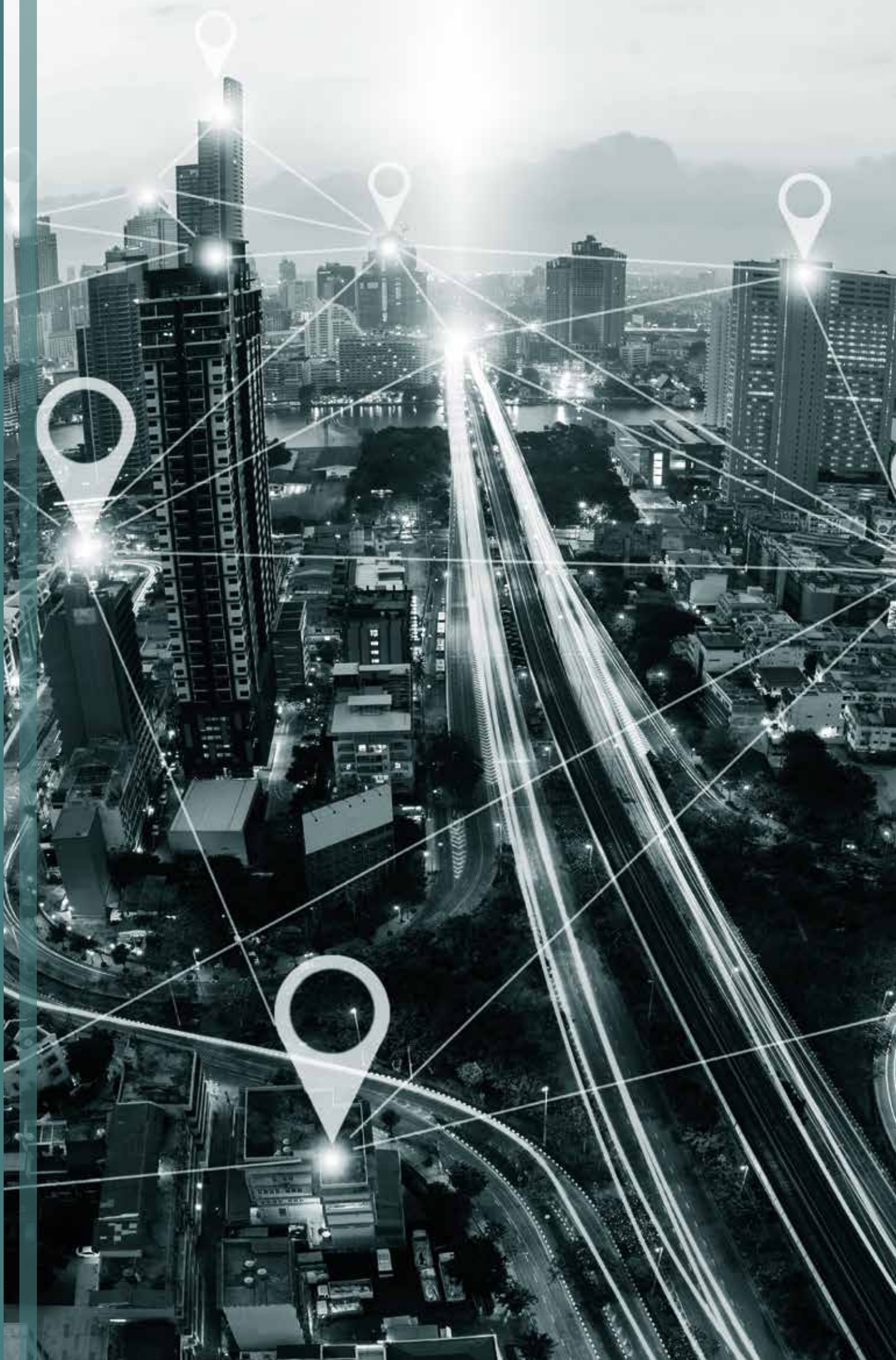
This survey highlights the range of views and challenges faced when implementing resilience programmes, whilst also reminding us that the concept is still finding its feet in many organisations and industries.

KEY FINDINGS

Resilience and the ability of an organisation to recover from disruptive events and to adapt to change is increasingly on the executive agenda – particularly given that 65% of respondents have experienced a disruption during the last 12 months and only 5% of respondents felt their organisation was highly capable of withstanding major disruptive events.

The importance of leadership in the implementation of resilience principles has been re-iterated, with over 53% of respondents indicating that effective leadership was the highest priority objective. More surprising, perhaps, is that 37% of respondents felt that their organisation lacked the staff with the relevant skills or talent to drive resilience forward; this is a rise of 17% on 2015 and of increasing concern to many clients. This in spite of the fact that 27% of respondents have actively recruited dedicated resources to support the resilience agenda.

- ISO 22316 providing guidance on resilience programmes. ISO 22316 provides guidelines for organisational resilience and 62% of respondents were either aware or have read this guidance. 92% of respondents agree with the core principles which focus largely on shared purpose and collaboration across functions. However, 18% of respondents indicated that they would not be striving to adopt the core principles preferring instead to stick to existing processes.
- The importance of effective leadership. 53% of all respondents indicated that the effectiveness of leadership was the highest priority objective supporting the resilience agenda. This aligns to the guidance in ISO 22316 which states effective management and governance supports organisational resilience. Anticipation of and managing change rated as the next highest priority for organisations. To build sufficient adaptability, resilience should be driven from the executive and management and should be embedded across the organisation.
- Lack of skills slows implementation down. Over one third (37%) of respondents felt that their organisations lacked the relevant skills or talent to drive resilience in their organisation; this is a rise of 17% on 2015 and of increasing concern to many clients. This is in spite of the fact that 27% of respondents have actively recruited dedicated resources to support the resilience agenda and 46% have invested in training, awareness, and communications.
- Companies are more worried about long-term reputational damage than short-term financial loss. Over 70% of respondents see reputational damage as the most significant concern to their business in the event of a disruption – considerably more than reduced revenue (38%), the loss of new business opportunities (25%), or reduced shareholder value (26%).
- Increasing concern over cyber threats. Respondents rated cyber security as the most potentially disruptive external threat to their organisation, with 47% stating this was their primary concern.
- 92% of respondents agree that cross-functional working and sharing of information is a key principle of resilience. However, 48% of respondents remain reliant on centralised governance and oversight instead of multi-disciplinary risk meetings that would perhaps encourage greater cross-functional collaboration and information sharing.

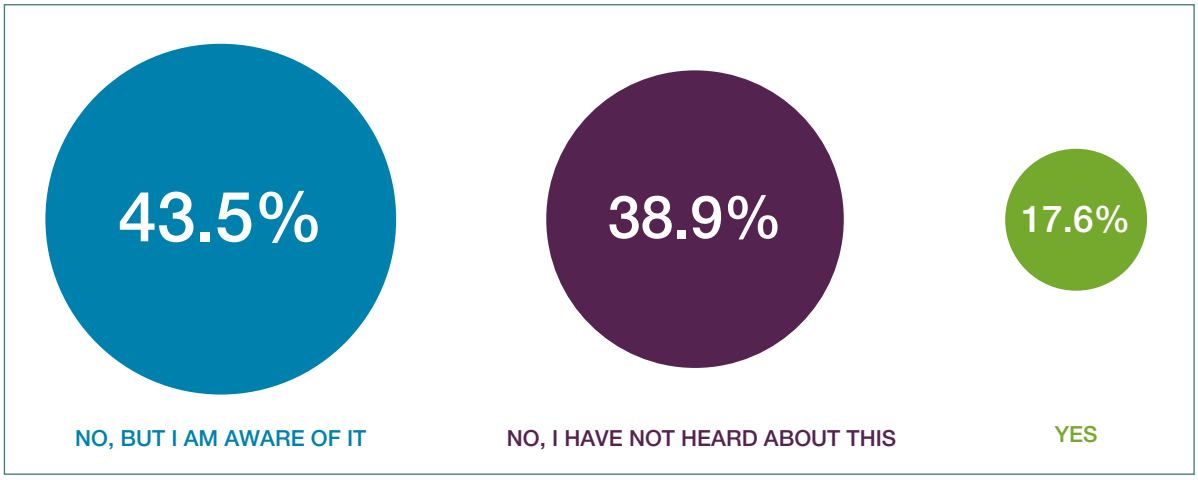


ANALYSIS

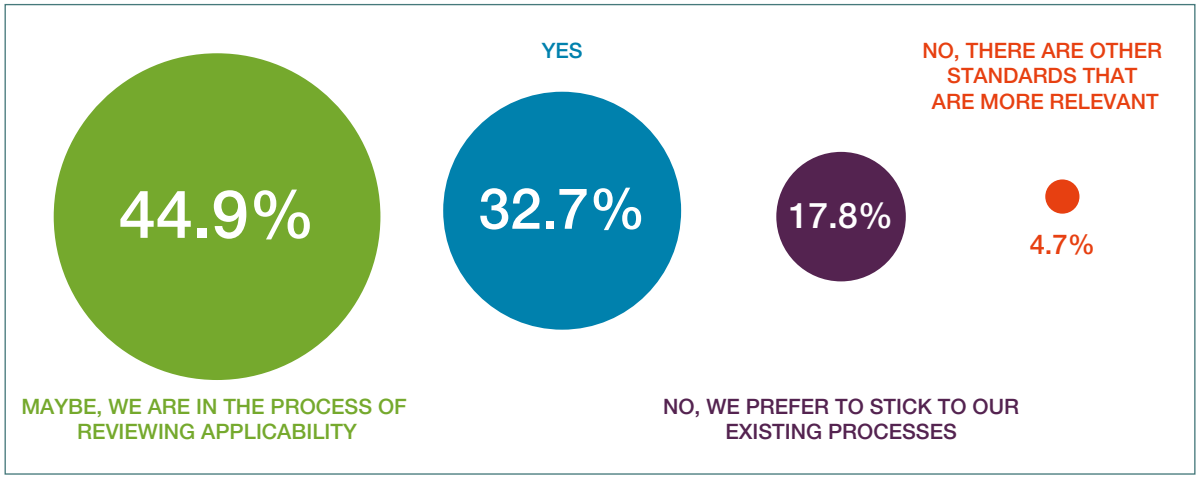
THE CHALLENGE OF MOVING FROM GUIDANCE TO IMPLEMENTATION

62% of respondents were either aware of, or have read, the ISO 22316 guidance. 92% of respondents agree with the core principles which focus largely on shared purpose and collaboration across functions. However, 18% of respondents indicated that they would not be striving to adopt the core principles, preferring instead to stick to existing processes. This perhaps provides some insight to the mind-set of many organisations that recognise the principles but challenge how the guidance set out in ISO 22316 translates into practical implementation.

Control Risks advocates developing resilience frameworks that span the enterprise, capturing and integrating existing risk management activities. The programme should be considered as a series of small projects that incrementally increase the resilience of the organisation over time. This is the approach adopted by a number of Control Risks' clients who address resilience as bite-sized projects, starting with a gap analysis, reviewing governance and reporting before subsequently building capability, thereby making building resilience more achievable and sustainable.



▲ Have you read the draft 'International Standard on Security and Resilience — Guidelines for Organisational Resilience (ISO 22316)'?



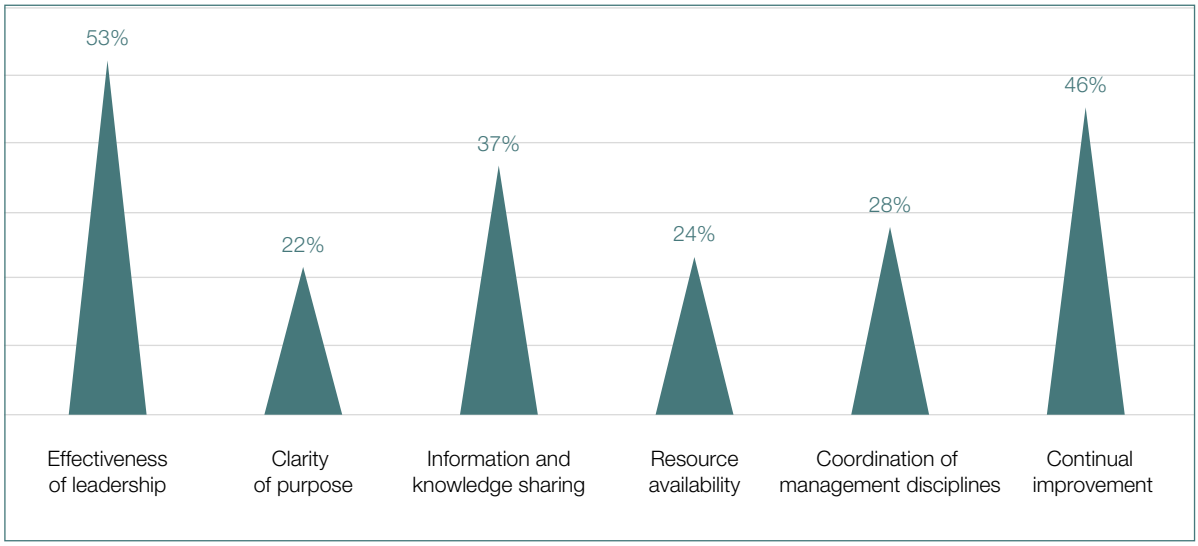
▲ Will you seek to align your business operations to the ISO guidelines for resilience when they are released?

THE IMPORTANCE OF EFFECTIVE LEADERSHIP

Organisations should be clear who is responsible and accountable for risk management including risk reporting, monitoring, and ownership. 53% of all respondents indicated that the effectiveness of leadership was the highest priority objective supporting the resilience agenda. Effective leadership drives the right culture and ultimately supports business strategy. Both culture and strategy need to be aligned to risk management processes whilst taking account of the risk acceptance of the organisation, all of which is a function of the organisational leadership.

There was unanimous agreement that responsibility for driving resilience lies with the executive. A point that is reiterated through ISO 22316: an organisation should empower leaders and 'encourage them to lead under a range of conditions and circumstances, including during periods of uncertainty and disruptions'.

When considering leadership in the context of resilience, organisations should reflect on what this means to them. In Control Risks' experience many leaders of organisations are superbly effective when the business is performing, but they may not be the most adept at managing change or disruption. Building experience and the capability of the organisational leadership to manage disruption is one solution; this may be in the form of planning, training or knowledge transfer with organisations with first-hand experience.



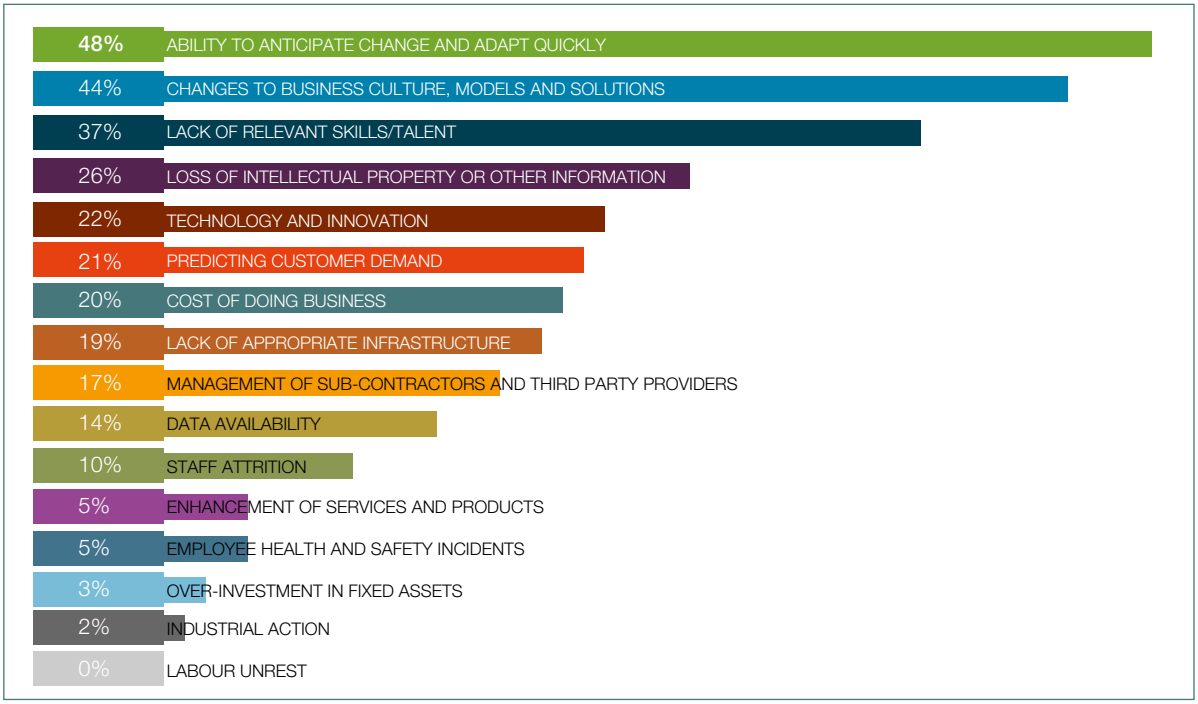
▲ Which of the following resilience objectives would your organisation classify as the highest priority?

LACK OF SKILLS IS SLOWING THE IMPLEMENTATION DOWN

Respondents are increasingly aware of the requirement to drive resilience through the increased collaboration of management disciplines. However, it appears as if many feel that their teams are under-resourced and lacking the right skills to engage across their organisations and drive the resilience agenda.

Somewhat surprisingly, 37% of respondents felt that their organisations lacked the relevant skills or talent to drive resilience in spite of the fact that 27% have actively recruited dedicated resources to support the resilience agenda. This points to challenges with interpreting the success factors of any resilience programme and highlights some of the challenges with the practical rollout of a resilience programme. Whilst the draft ISO 22316 provides some guidelines for organisational resilience, there still needs to be thought applied to how this translates into something tangible for organisations to prove that they are meeting their resilience objectives.

Organisations should consider building the capability of their personnel with essential skills such as the ability to collaborate, communicate, and build cohesion alongside the relevant competencies to interpret the resilience requirements. This would support the effective delivery of the organisational strategy whilst enabling sufficient flexibility to respond to changing circumstances.



▲ What do you consider to be the most disruptive internal threats to your organisation's business over the next 5-10 years?

COMPANIES ARE MORE WORRIED ABOUT LONG-TERM REPUTATIONAL DAMAGE THAN SHORT-TERM FINANCIAL LOSS

In light of a number of recent high-profile reputational crises such as those involving TalkTalk[1] and VW, over 70% of respondents see reputational damage as the most significant concern to their business in the event of a disruption – considerably more than reduced revenue (38%), loss of new business opportunities (25%), or reduced shareholder value (26%). It is estimated that the financial impact to TalkTalk was $80m and to VW a staggering $15bn, meaning that organisations are increasingly and rightly concerned about reputation and maintaining market share in the event of such crises.

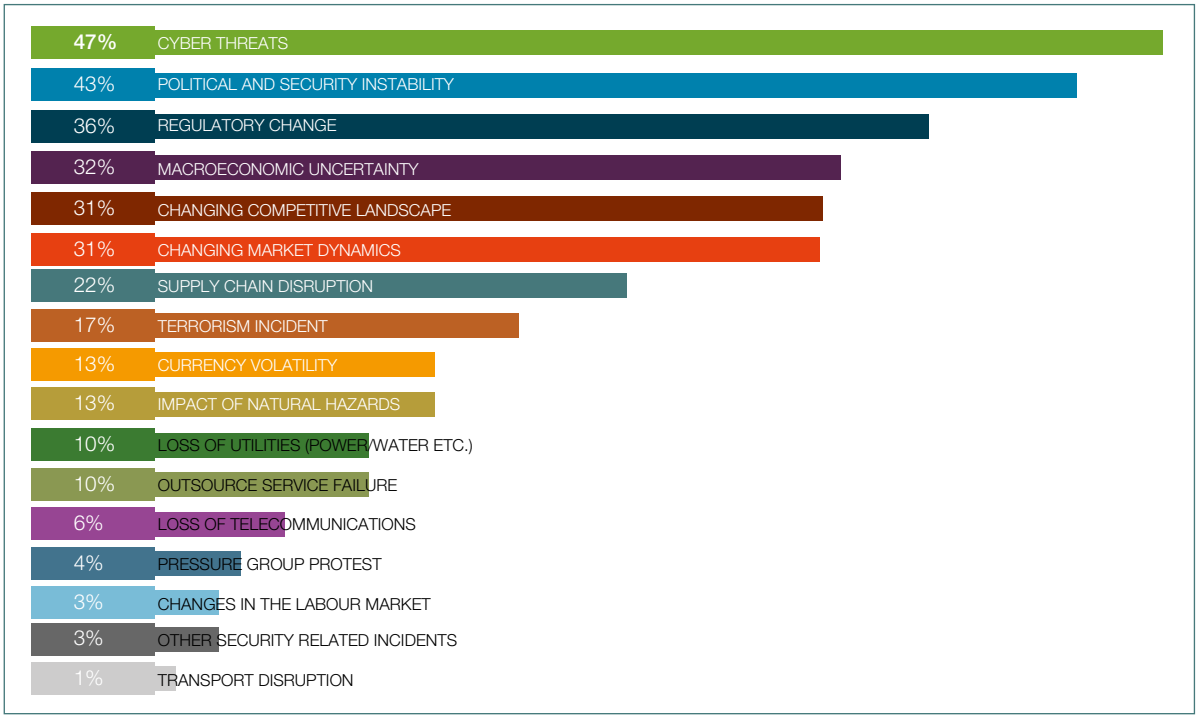
▲ Which impact would be of most concern to your business?

1 | A massive cyberattack against ISP TalkTalk saw 150,000 customer details swiped in October 2015, costing the company £60 million and the loss of 95,000 customers.

As organisations increasingly seek to become more resilient they are looking to ensure that they can weather short-term financial shocks and other disruptions. Concerns over long-term reputational damage could be linked to a sense of inappropriate structures and resources to manage disruptions as they occur. Every organisation seeks to maintain its reputation and integrity to support long-term success, and where there is a failure to do this it is normally attributed to being unable to adapt and effectively manage the disruptive event.

INCREASING CONCERN OVER THE CYBER THREAT

In 2016 almost half of all respondents (47%) believed the most disruptive external threat to their organisation was cyber related. This compares to the majority of respondents in 2015 believing that the impact of political instability posed the biggest threat (62% of respondents). Linked to this increasing awareness of the cyber threat was a noticeable increase in concern over the loss of data and intellectual property.



▲ What do you consider to be the most disruptive external threats to your organisation's business over the next 5-10 years?

For many years a range of international and national public and private sector organisations have pointed to cyber threats as being extremely serious for most organisations. The results of this survey are likely to indicate several factors:

- Companies are now recognising the severity of cyber threats
- Many companies may have been victims of a cyber attack over the last year as the volume of cyber breaches continues to grow

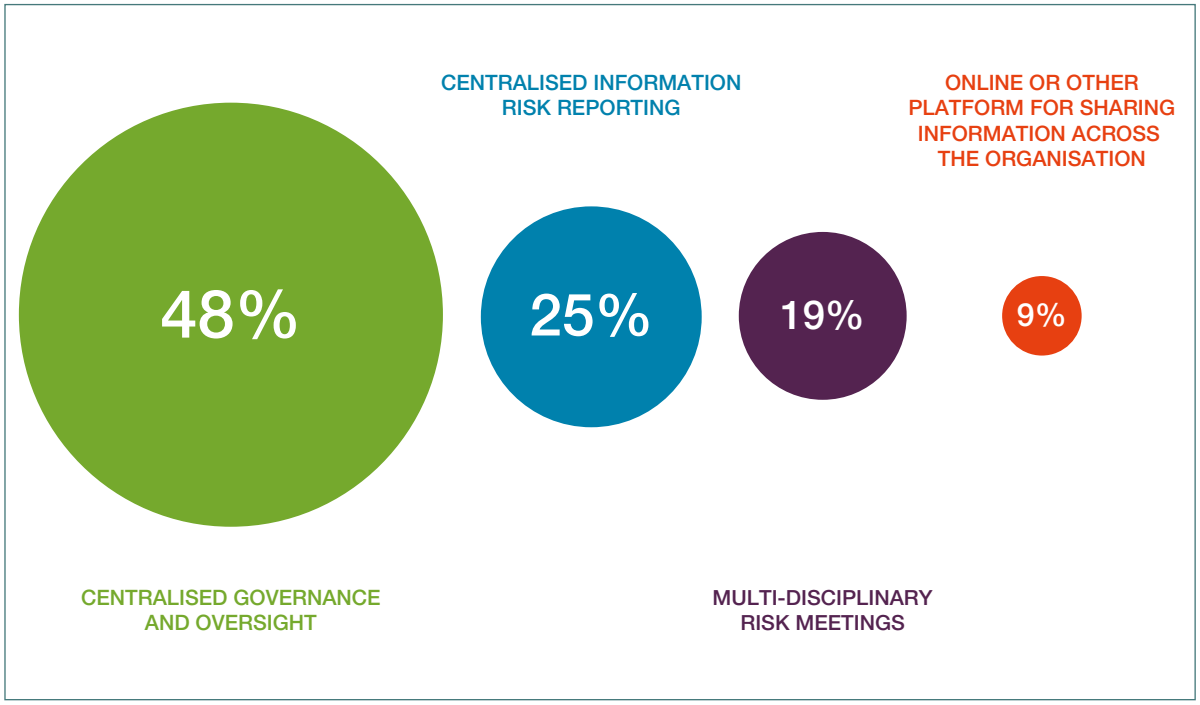
Over the last twelve months, Control Risks has seen many clients adapting to the increased political and security instability and updating their risk monitoring and mitigation plans. But they have recognised that they do not yet fully understand the nature and extend of the cyber threat they face, ranking cyber threats higher than other external threats. Companies are not yet sure on how to best manage this complex, powerful, and evolving risk to their business.

Results also suggest that organisations are then prioritising external cyber threats and potentially failing to examine and address some of the key issues relating to insider threats.

It is recognised that insiders and third parties pose security risks due to their legitimate access to facilities and information, knowledge of the organisation and the location of valuable assets. Insiders will know how to achieve the greatest impact whilst leaving little evidence. This cyber threat is often overlooked in favour of the more heavily 'promoted and visible external hacker threats'. It also raises uncomfortable questions regarding loyalty and betrayal within an organisation's security in the context of organisational and cultural factors, and changing economic and social factors; all of which are important in the context of building organisational resilience.

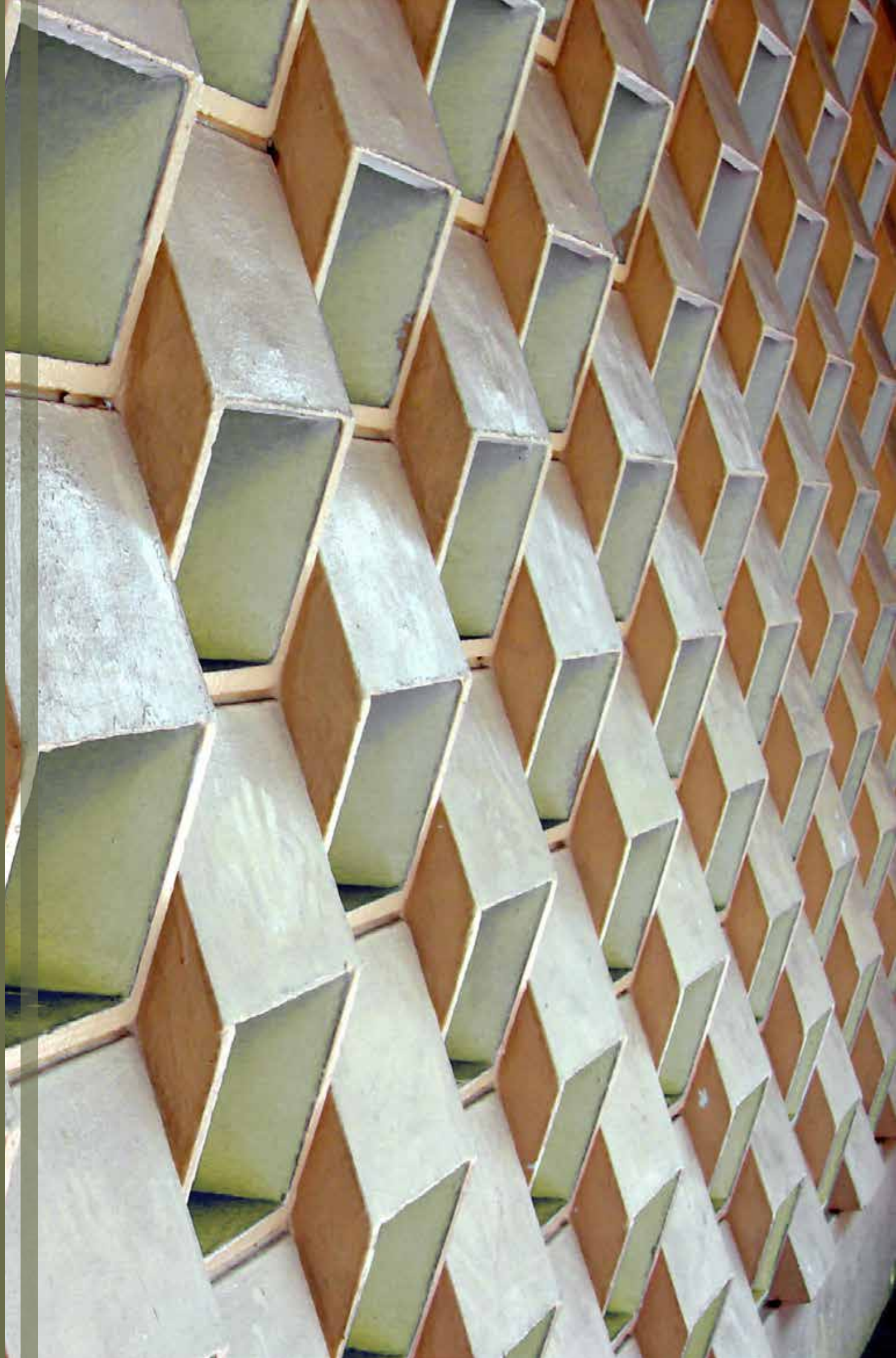
PRINCIPLES OF RESILIENCE

A key principle of resilience is based on cross-functional working and sharing information. 92% of respondents agree with the core principles of resilience, but 48% of respondents remain reliant on centralised governance and oversight instead of multi-disciplinary risk meetings that would encourage greater cross-functional collaboration and information sharing.



▲ What does your organisation do to encourage resilience management disciplines (strategic planning, financial planning, risk management, business continuity management, crisis management and security management) to work cross functionally?

To encourage cross functional collaboration and information sharing organisations should not only emphasise the values they are looking to drive, thereby aligning employees around the organisational strategy and approach to resilience, but they should also consider the risk governance and reporting arrangements within their organisations. Changes to working practices may actively encourage greater information sharing and collaboration, driving increased organisational resilience through providing greater visibility and warning of potential risk events.



CONCLUSION

The threat from disruptive events has encouraged clients from all sectors to consider specific threats to their operations and identify areas of vulnerability. It is clear that many organisations are focussed on the need to become more resilient, but the implementation of the strategies and tactics that support this is currently lacking.

There is widespread recognition that building resilience requires organisation-wide action. It is only through the continued engagement with senior leadership that the appropriate capacity, capability, plans and controls can be put in place to reduce organisational risk exposure to disruptive events.

To build a resilient organisation the emphasis should not purely be on strategy, or the culture of the organisation, or the way it handles risk management. A resilient organisation is one where these three components integrate to achieve the desired effect. Resilience is as much about the tangible strategy and processes as it is about the softer cultural requirements.

KEY RECOMMENDATIONS

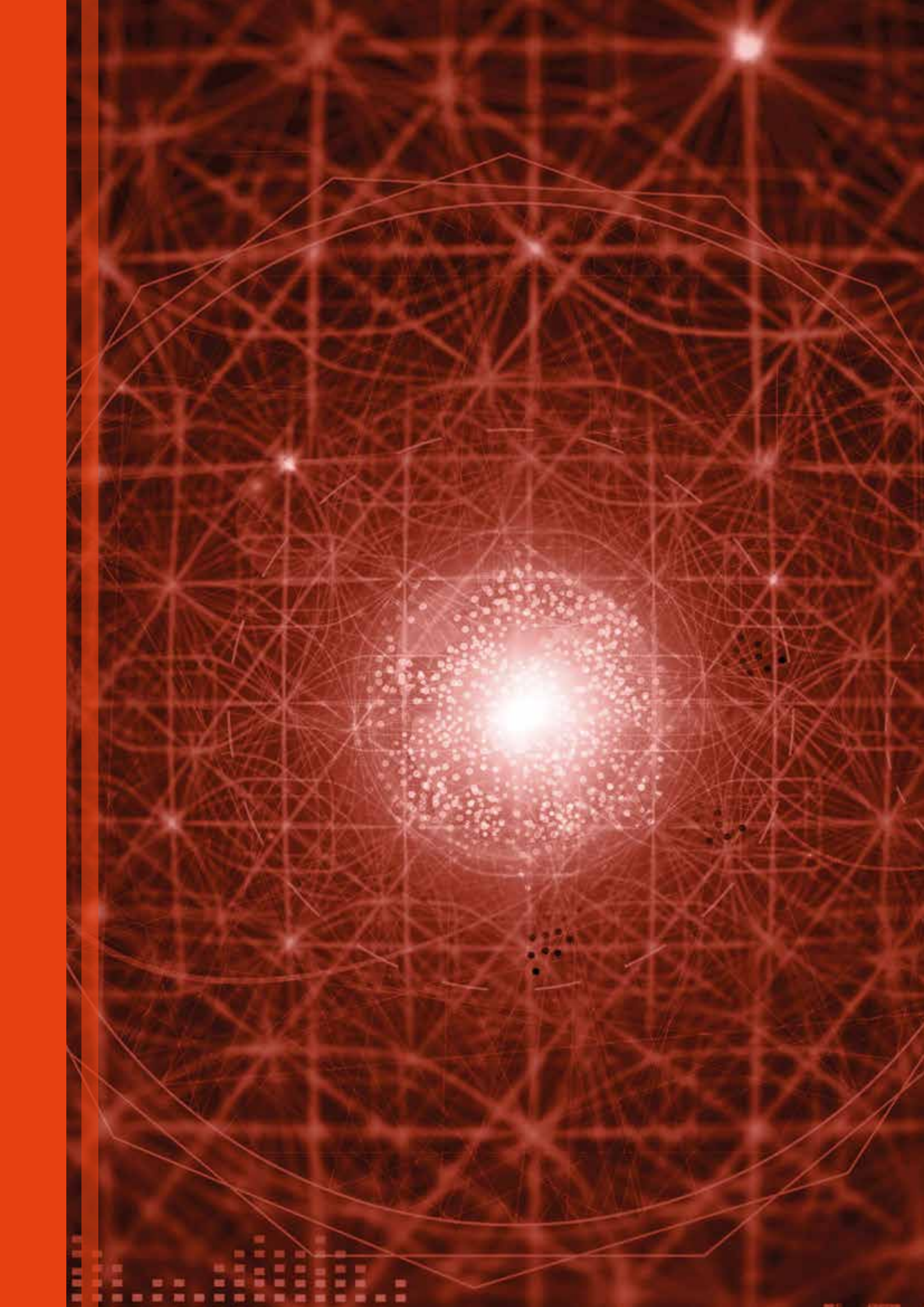
The top four key recommendations from the survey are as follows:

1. **Develop resilience frameworks that span the enterprise, capturing and integrating existing risk management activities. A resilience programme should be considered as a bundle of small projects that incrementally increase the resilience of the organisation over time.**
2. **Integrate the risk management activities and operational disciplines, thereby ensuring that knowledge is actively shared across internal organisational boundaries; consider the utility of multi-disciplinary risk meetings to encourage greater cross-functional collaboration and information sharing.**
3. **Build the capability of personnel with the essential skills such as the ability to collaborate, communicate and build cohesion alongside the relevant competencies to interpret and implement the resilience requirements.**
4. **Organisations should update their cyber risk monitoring and mitigation plans, doing everything they can to manage this complex, powerful, and evolving risk to the business.**

CONTACT THE AUTHORS:

Mark Whyte, Senior Partner, mark.whyte@controlrisks.com

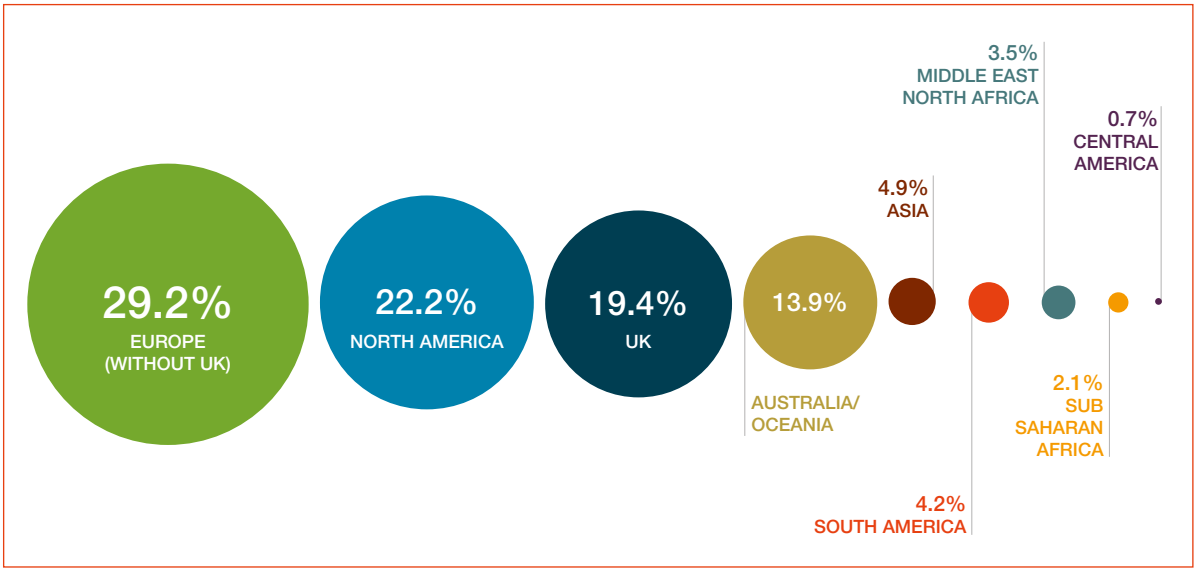
Andy Cox, Director, andy.cox@controlrisks.com



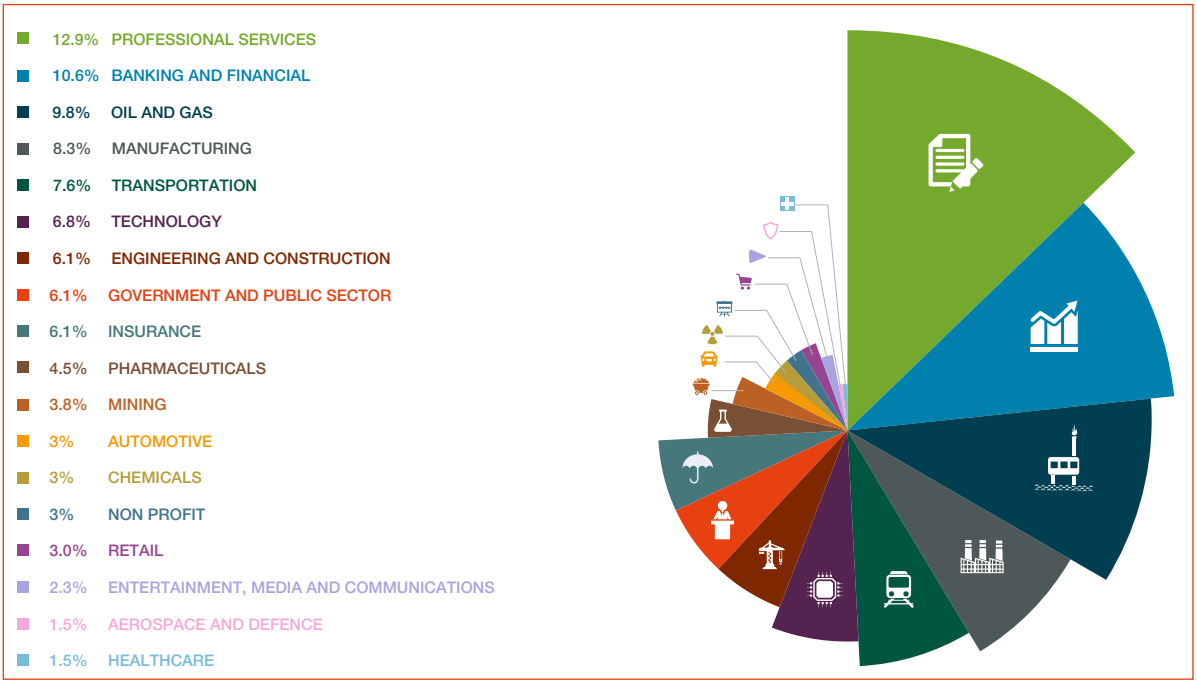
ABOUT THE SURVEY

With an increasing focus on the development of resilience this global survey was commissioned to receive feedback from our clients and our contact base on their progress and challenges in implementing the concept of resilience. This global survey, conducted between June and August 2016, took the opinion of 144 respondents into account.

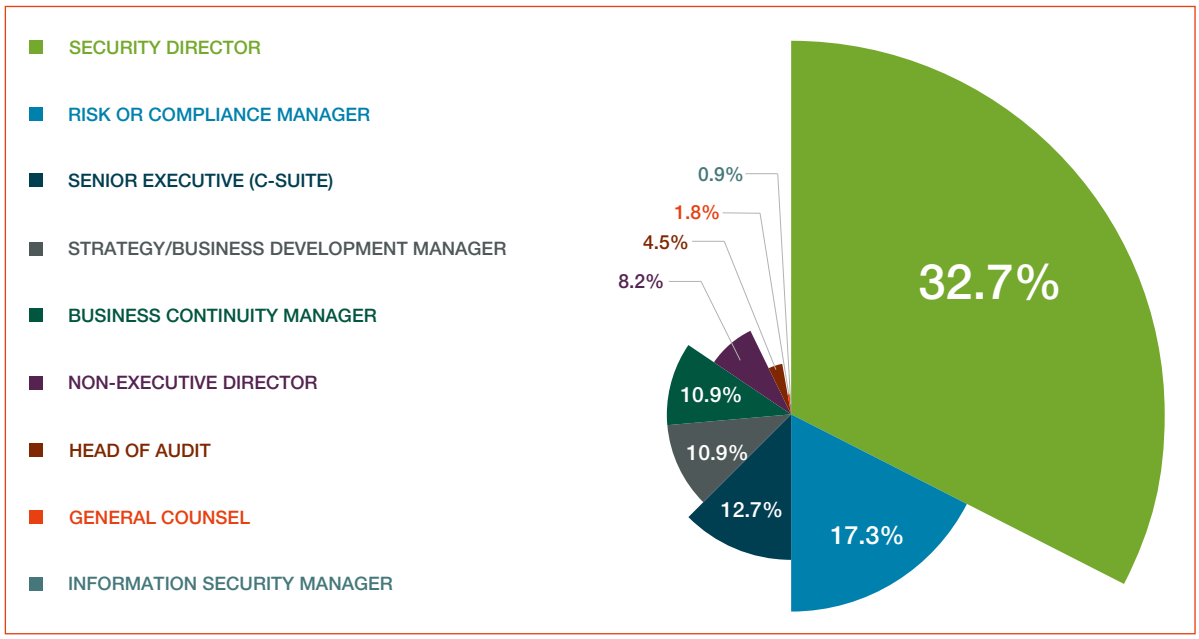
While there was a geographical focus on Europe, we had respondents from across the globe, representing all major industries.



▲ In which region are your headquarters located?



▲ Which of the following best describes the industry of your organisation?



▲ What is your job title?

ABOUT CONTROL RISKS

Control Risks is an independent, global risk consultancy specialising in helping organisations manage political, integrity and security risks in complex and hostile environments. Since 1975, we have worked in over 130 countries for more than 5,500 clients. With 37 offices on 5 continents our global reach ensures we are always close to where our clients need us. We support clients by providing strategic consultancy, expert analysis and in-depth investigations, handling sensitive political issues and providing practical on-the-ground protection and support.

Our unique combination of services, geographical reach and the trust our clients place in us ensure we can help them to effectively solve their problems and realise new opportunities across the world.

Control Risks have been supporting clients build organisational resilience with the capability to anticipate, prepare for, respond to and recover from disruptive events. We have developed both preventative strategies and adaptive capacity in client organisations to enhance their resilience.

Robust resilience relies on an organisation's behaviours, mechanisms and processes. Identifying crucial gaps or vulnerabilities in the organisational approach to threat identification and management helps shape strategy, crisis management and business continuity planning – building an organisation's resilience. A risk assessment identifies an organisation's crucial assets and business processes, and tests these against a set of five criteria:

- Robustness: its inherent strength and ability to resist threats
- Redundancy: properties that allow for alternative options
- Resourcefulness: capacity to mobilise needed resources
- Response: the rapidity with which it responds to a disruptive event
- Recovery: its ability to return to previous or improved operating standards

If you want to learn more about Control Risks' resilience support, please contact us at enquiries@controlrisks.com.

Control Risks' offices

abudhabi@controlrisks.com
alkhobar@controlrisks.com
amsterdam@controlrisks.com
baghdad@controlrisks.com
basra@controlrisks.com
beijing@controlrisks.com
berlin@controlrisks.com
bogota@controlrisks.com
chicago@controlrisks.com
copenhagen@controlrisks.com
delhi@controlrisks.com
dubai@controlrisks.com
erbil@controlrisks.com
frankfurt@controlrisks.com
hongkong@controlrisks.com
houston@controlrisks.com
jakarta@controlrisks.com
johannesburg@controlrisks.com
lagos@controlrisks.com
london@controlrisks.com
losangeles@controlrisks.com
mexicocity@controlrisks.com
moscow@controlrisks.com
mumbai@controlrisks.com
nairobi@controlrisks.com
newyork@controlrisks.com
panamacity@controlrisks.com
paris@controlrisks.com
portharcourt@controlrisks.com
saopaulo@controlrisks.com
seoul@controlrisks.com
shanghai@controlrisks.com
singapore@controlrisks.com
sydney@controlrisks.com
tokyo@controlrisks.com
washington@controlrisks.com

www.controlrisks.com