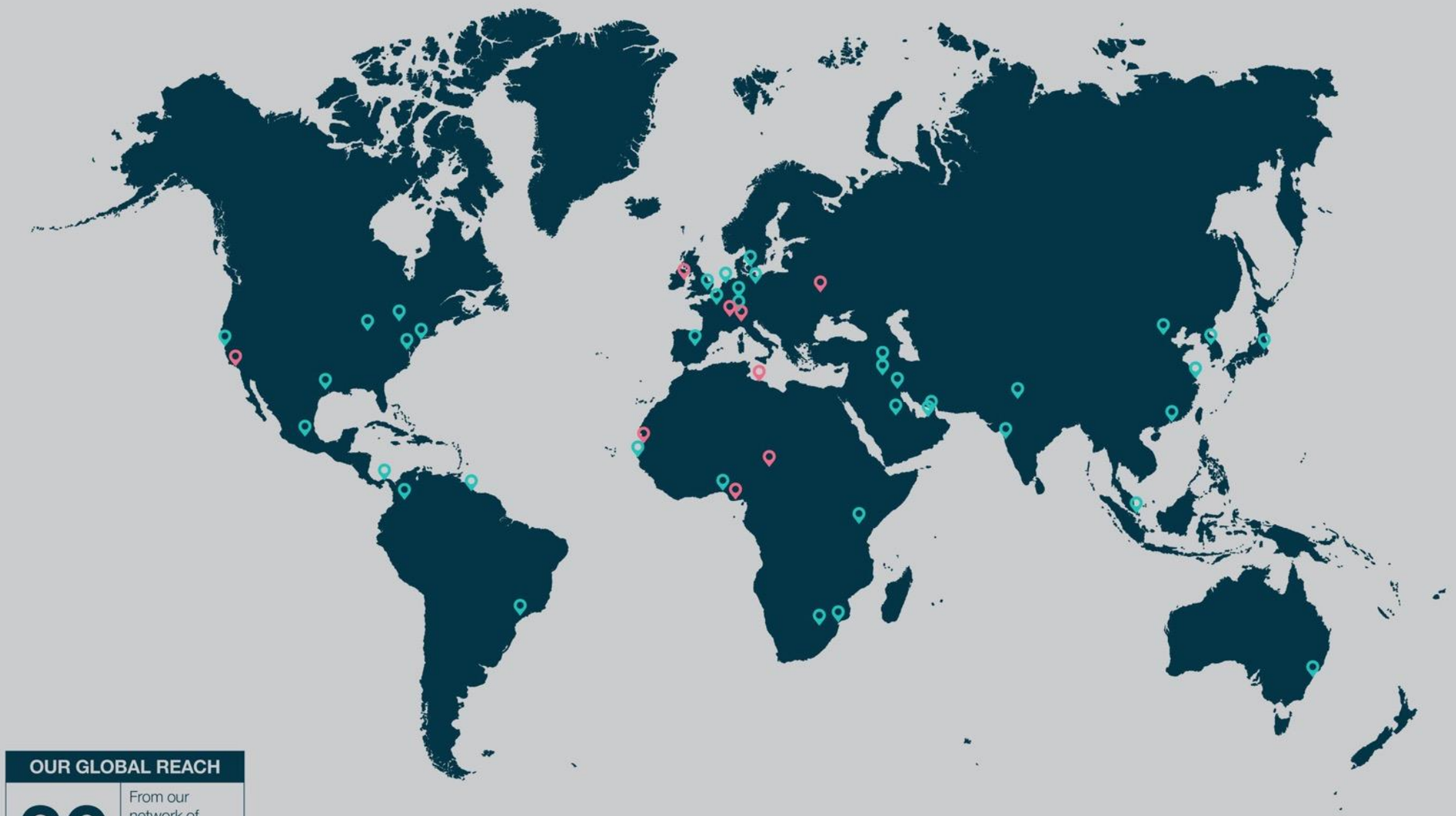
August 2024

Strengthening Resilience – Polycrisis

Prepared by Control Risks
Mark Shortman – Partner, and Head of Crisis & Security Practice
Jon Greenaway – Market Director



Global offices

Americas

Bogotá
Chicago
Georgetown
Houston
Mexico City
New York City
Panama City
San Francisco
São Paulo
Toronto
Washington DC

Asia Pacific

Beijing
Delhi
Hong Kong
Mumbai
Seoul
Shanghai
Singapore
Sydney
Tokyo

Europe, Middle East and Africa

Abu Dhabi
Amsterdam
Baghdad
Basra
Berlin
Copenhagen
Dakar
Dubai
Erbil
Frankfurt
Johannesburg
Lagos
London
Madrid
Maputo
Nairobi
Paris
Riyadh
Zurich

Representations

Americas

Los Angeles

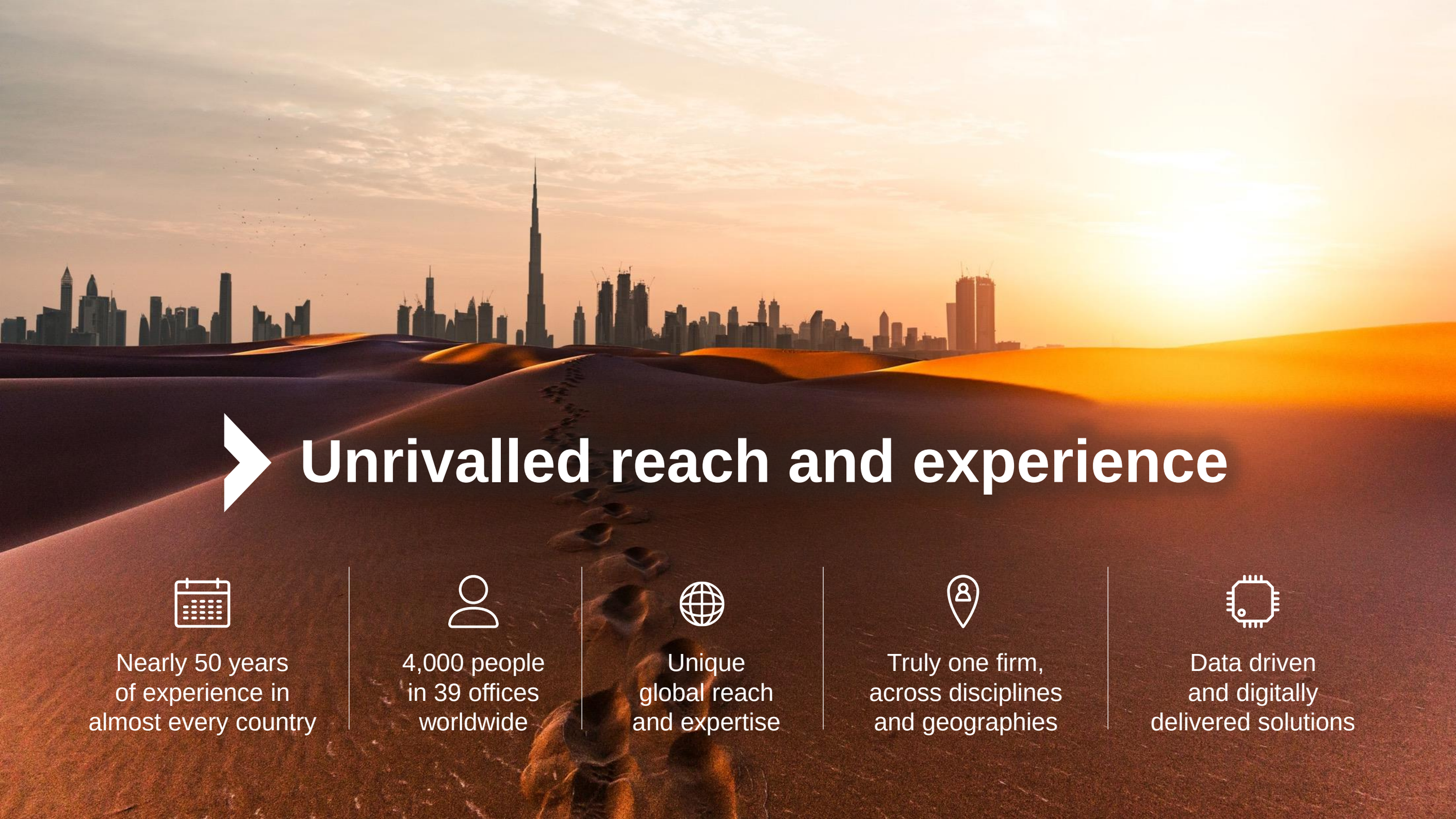
Europe, Middle East and Africa

Dublin
Geneva
Kyiv
Milan
N'Djamena
Nouakchott
Port Harcourt
Tripoli

OUR GLOBAL REACH

39 From our network of 39 offices, we work wherever you need us.

MAP CORRECT AS OF APRIL 2024



Unrivalled reach and experience

Nearly 50 years of experience in almost every country

4,000 people in 39 offices worldwide

Unique global reach and expertise

Truly one firm, across disciplines and geographies

Data driven and digitally delivered solutions

Introduction

Control Risks' understanding of resilience:

"A resilient organisation is one that understands its operating environment in the broadest sense, grasp the inherent risks and opportunities, appropriately manages its risks and, if things go wrong, are able to respond and adapt effectively to emerge stronger".

The aim of the Global Resilience Survey is to better understand how organisations are implementing resilience programmes in practice and adapting the principles of resilience in the face of progressively more intensive crises.

“Resilience is a construct, not a product”

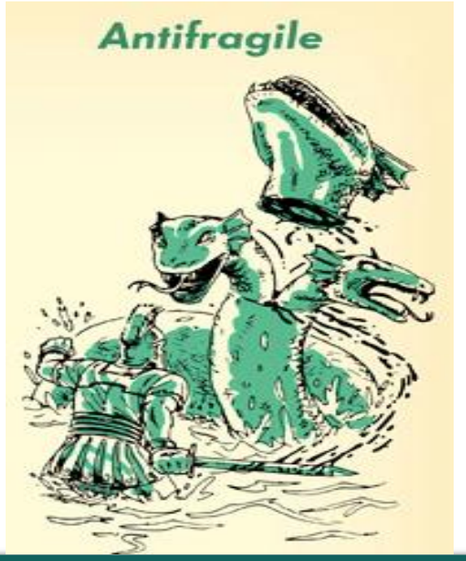
The resilience pendulum

Fragile

- Suffers or breaks from volatility
- More downside than upside from volatility
- Seeks tranquility
- **Myth: Sword of Damocles**

Resilient

- Stays the same in volatility
- Re-emerges the same
- **Myth: Phoenix**



Anti-Fragile

- Grows and gets stronger with volatility
- More upside than downside from volatility
- Seeks disorder
- **Myth: Hydra**

Typical conversations about resilience

- **Business resilience:**

  Is the **"***traditional approach to strengthening an organisation's ability to prepare, respond and recover from acute crisis and disruption.***"**

- **Operational resilience:**

  By **"***Anticipating and dealing with disruption, through effective integration and coordination of enterprise-wide risk controls, response measures, and all elements of operations, technology and supporting functions"*

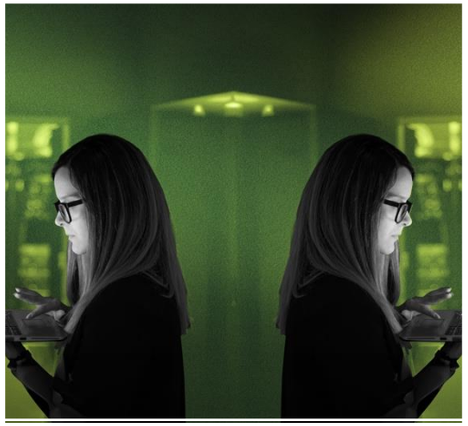
- **Organisational resilience:**

  Is the *"effective execution of our company strategy despite facing an ever changing business and operating environment, by centrally dealing with uncertainty and change with clear intent, organisational coherence, with leadership participation and appropriate resourcing***"**.

The 2024 global risk landscape

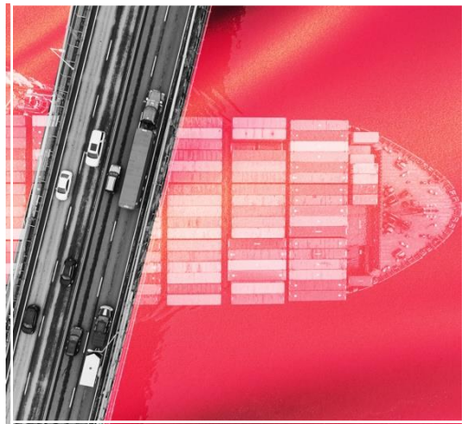
RISK MANAGEMENT OVERLOAD: CRISIS EVERYWHERE

In 2024, the sheer number and diversity of crisis events anticipated is testing the capability of organisations to adapt and manage more frequent and complex scenarios.



TRUST DEFICIT: DIGITAL INTEGRITY FRAYS

Companies across the world are confronted by a paradigm shift in the integrity and resilience of the data, systems and technologies on which their businesses rely.



THE GREAT REALIGNMENT: ACTING GLOBALLY SURVIVNG LOCALLY

As countries realign and reorient, global businesses will need to pay attention to the individual interests of a wider range of stakeholders.

UNCERTAINTY PARALYSIS: US POLITICS AND CHINA'S ECONOMY

China and the United States are drifting further apart as they face economic and domestic challenges that will add enormous complexity to any strategic plans.

CLIMATE DISRUPTION: THE GLOBAL THREAT MULTIPLIER

The need for many businesses to catch up on their climate adaptation needs has never been more pressing, exacerbating and accelerating other disruptive events.

Control Risks: 2024 Global Risk Landscape

2024 Polycrisis nexus

*The nexus between resilience and polycrisis underscores the importance of a **holistic and integrated approach** to crisis management and response. Organizations that successfully navigate polycrisis exhibit a combination of **strategic foresight**, **adaptability**, and a **commitment to continuous improvement***

2024 may well witness a high-water mark in…

- Complexity
- Chain reaction and residual risks
- Global conflicts
- Shifting geopolitics
- Speed of technology
- AI & sophistication
- A shifting emphasis towards Readiness, and ease the response and recovery costs
- Boards relationship with “resilience” and formal Director obligations

Polycrisis - *"Different risk events compound their effects, potentially overwhelming the capacity of individuals, organisations, or systems to respond effectively"*

- Not linear
- Not singular in nature
- More protracted, in months & years
- Existential, shareholder value
- More sophisticated
- More costly
- Enemy of brands and reputations
- Highly publicized
- Duty of care
- Anxious Boards

COVID-19 Pandemic (Health and Economic Crisis):
Pandemic created global health crisis, and its economic implications were significant, impacting industries, employment, and global supply chains.

Climate Change (Environmental and Social Crisis):
Environmental challenges, including extreme weather events, rising sea levels, and biodiversity loss, have social, economic, and political implications.

Global Economic Inequality (Economic and Social Crisis):
Disparities in wealth distribution and economic opportunities contribute to social and political tensions globally.

Cybersecurity Threats (Technological and Security Crisis):
Increasing cyber threats, including ransomware attacks and data breaches, pose risks to individuals, businesses, and governments worldwide.

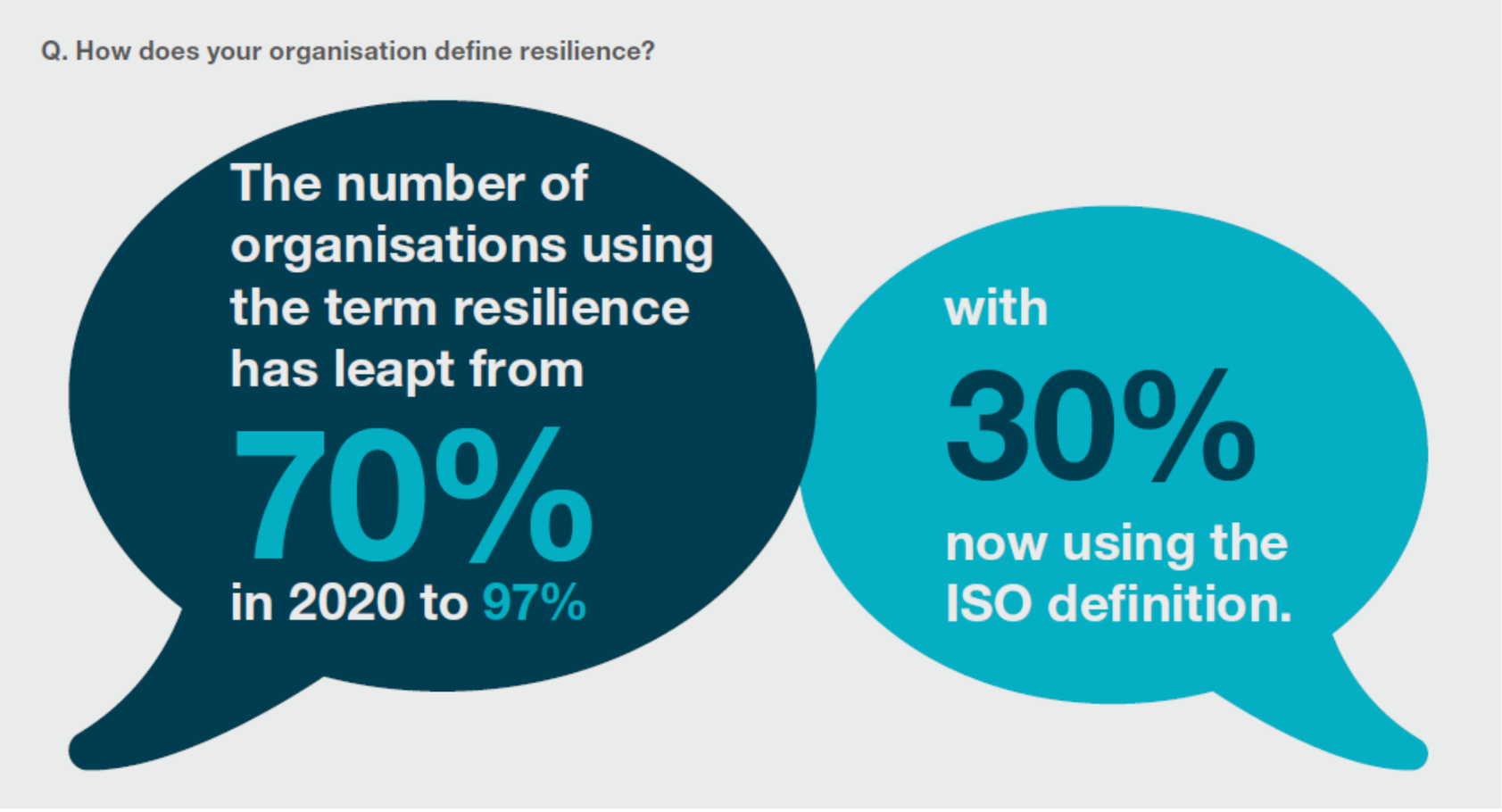
Political Instability and Conflicts (Political and Security Crisis):
Ongoing political instability and conflicts in various regions can lead to humanitarian crises and displacement of populations

Humanitarian Crises (Refugee Crisis, Famine):
Various regions face humanitarian challenges due to conflicts, natural disasters, or other factors, leading to displacement and food insecurity

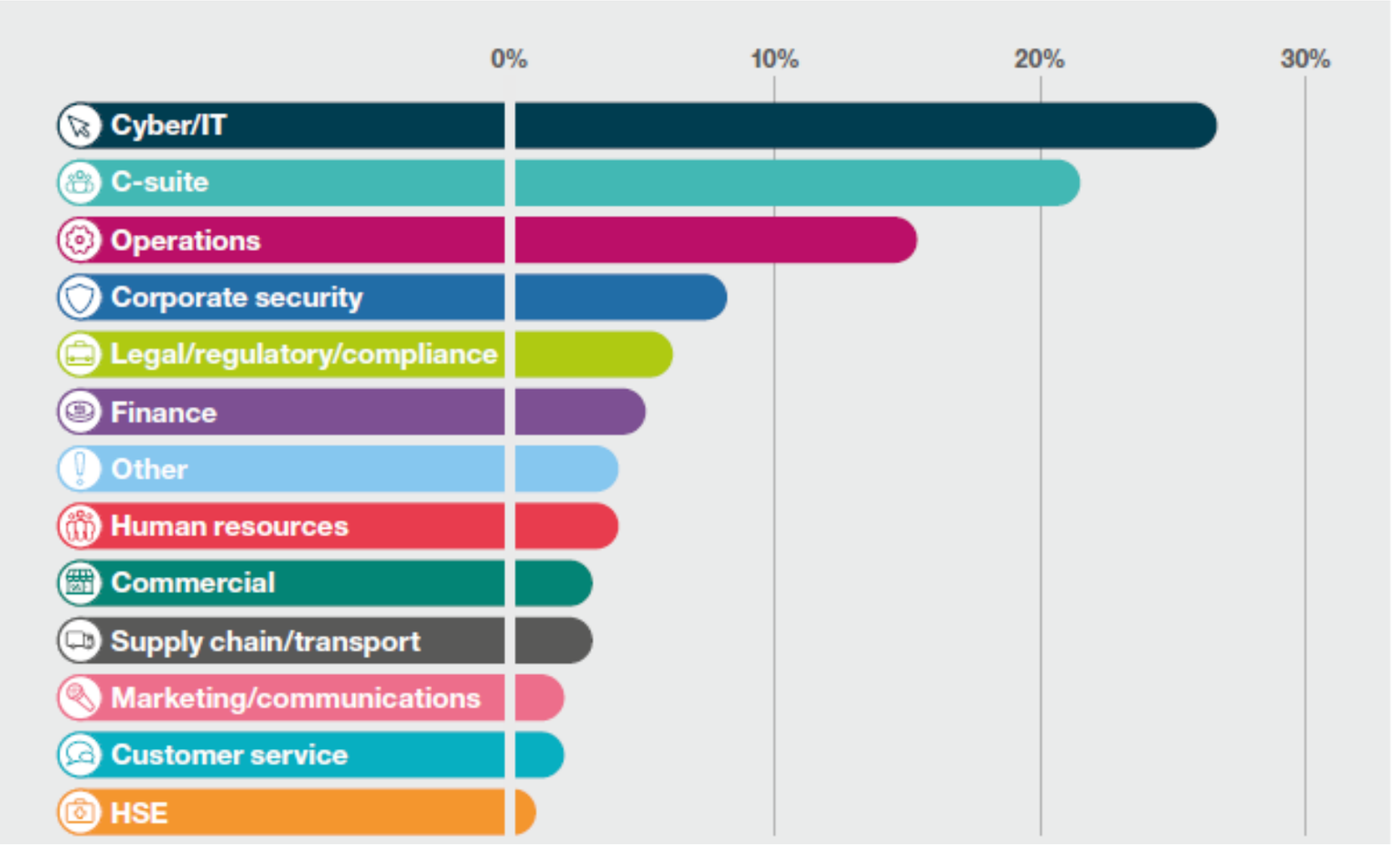
Polarization and Social Unrest (Social and Political Crisis):
Growing social and political polarization in some countries has led to increased social unrest and challenges to governance.

Public Health Emergencies (Beyond COVID-19):
Other infectious diseases, disease X, antibiotic resistance, and healthcare system challenges contribute to ongoing public health concerns.

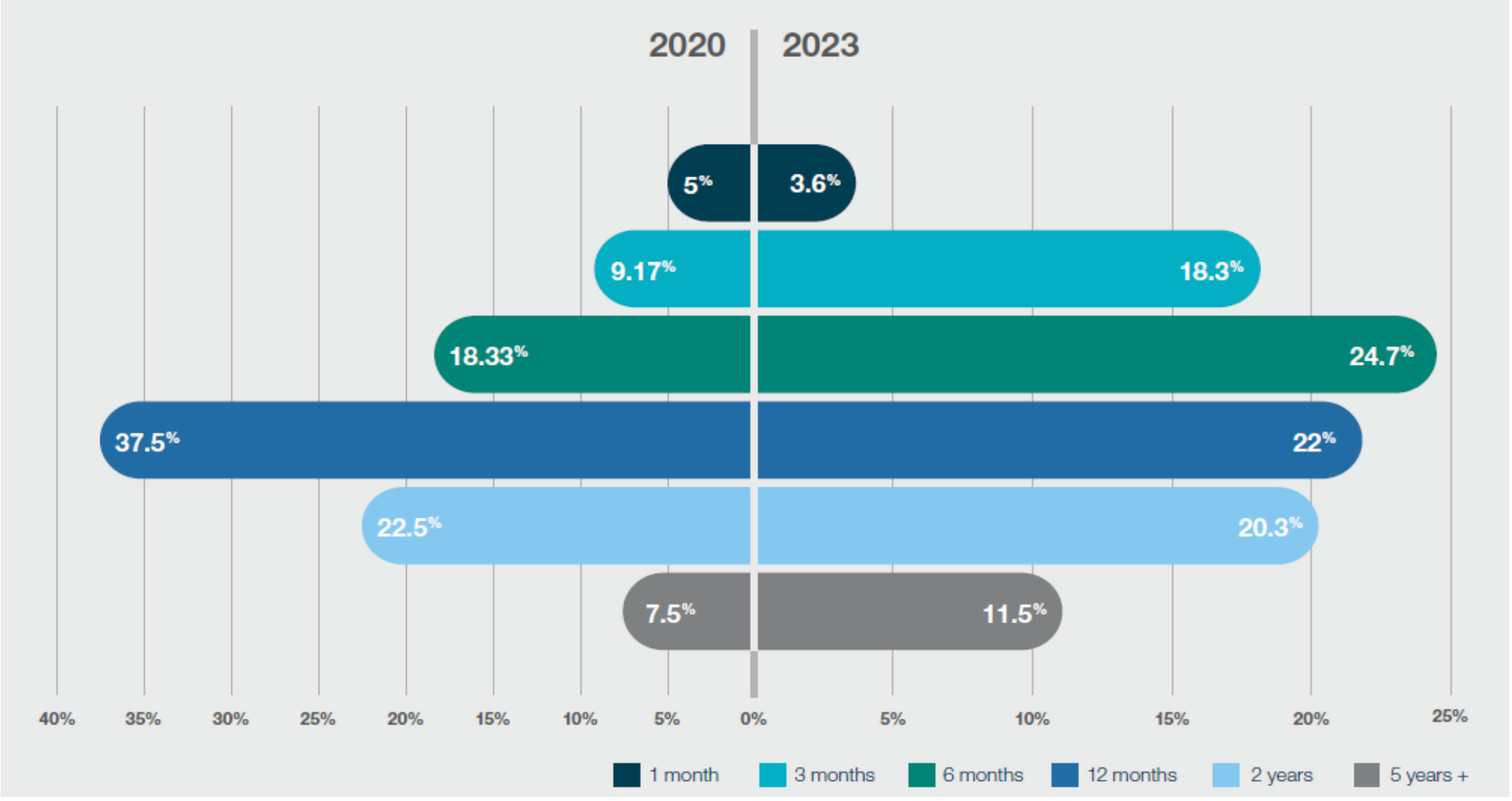
Resilience


Q. How does your organisation define resilience?
The number of organisations using the term resilience has leapt from
70%
in 2020 to 97%
with
30%
now using the ISO definition.

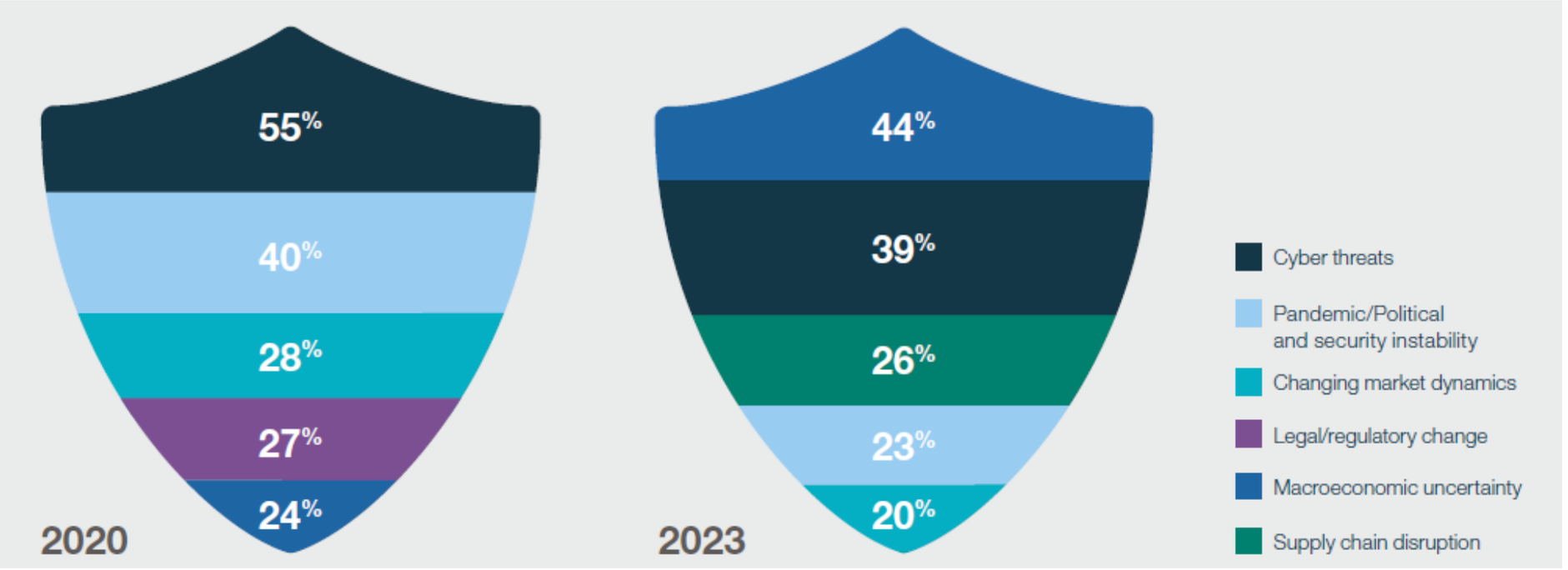
Which function owns resilience in your organisation?



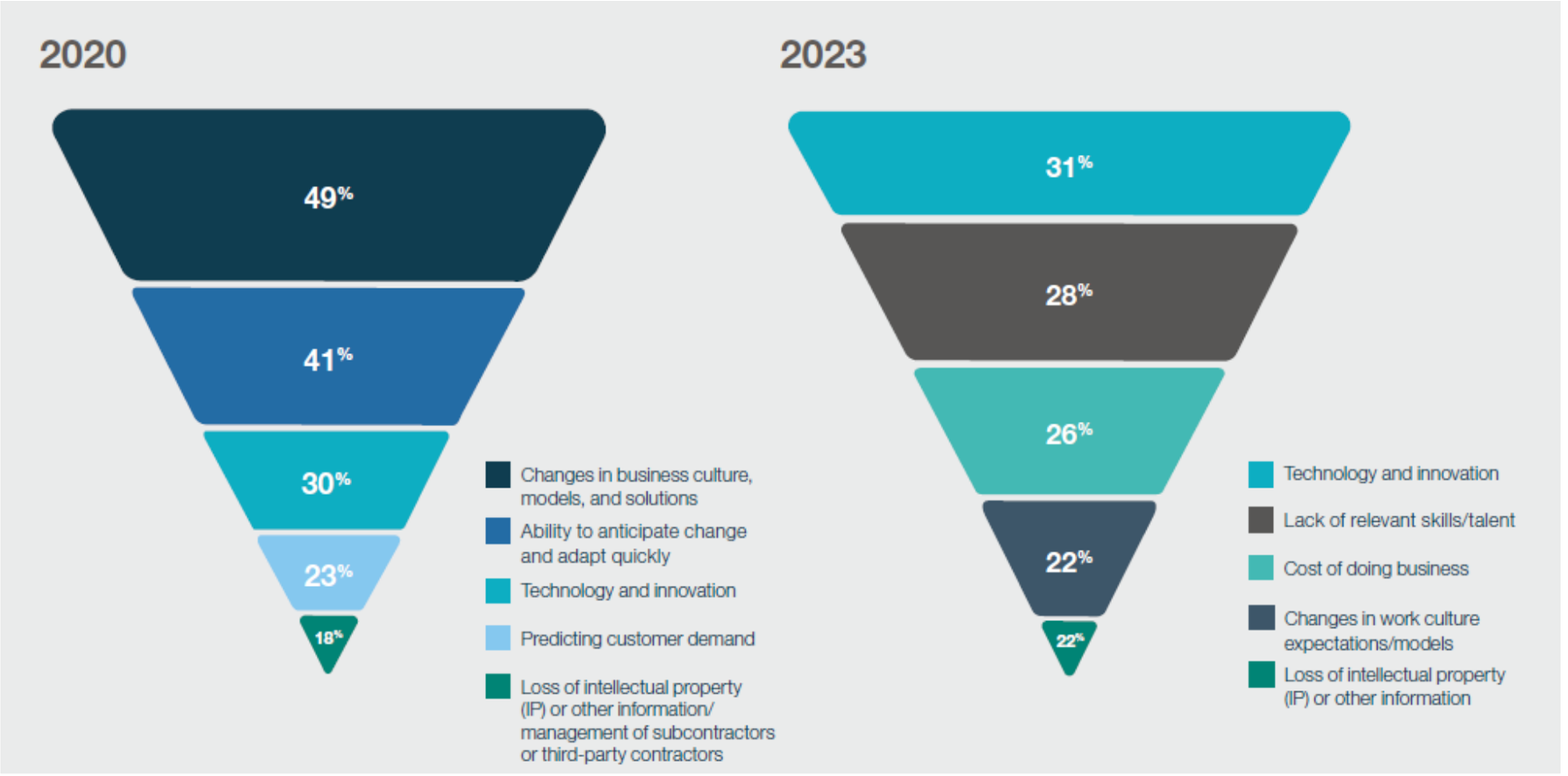
How far ahead of time does your organisation monitor and analyse risk?



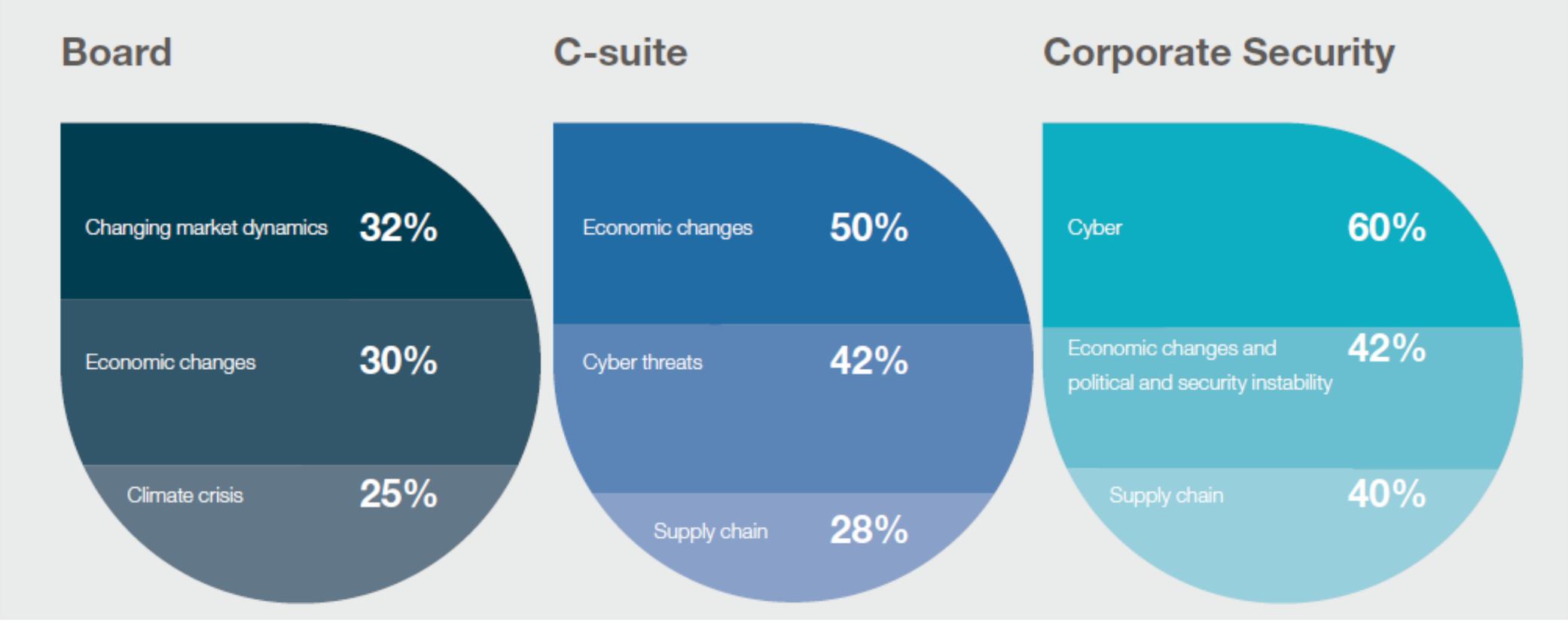
What do you consider to be the most disruptive external threats to your organisation's business over the next 5-10 years?



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



Different functional perspectives on the most disruptive internal threats to their organisation's business over the next 5-10 years



Insights from other organisations: organisational investment to increase capability and capacity

Q: Survey participants were asked to select all that apply. Given your experience, where is your organisation investing to increase capacity and capability?

Control Risks: Global Resilience Survey 2020 & 2023

Digital integrity | Global cyber threat landscape

US authorities warn that China-linked actors are conducting **pre-positioning** operations likely to facilitate **disruptive attacks** in event of escalation
May 2023

German citizen **arrested for espionage** for sharing information with Russia that he acquired in his position at Germany's Office for Equipment, Information Technology and Utilization (BAAINBw)
August 2023

Russia-aligned cyber activists and cybercriminals launch **highly disruptive** attack against German manufacturing organisation in response to Germany supporting Ukraine
April 2023

North Korea's compromise of 3CX first known **cascading supply chain compromise**
April 2023

Ransomware attack on Japan's Port of Nagoya halts operations, delays import and exports
September 2023

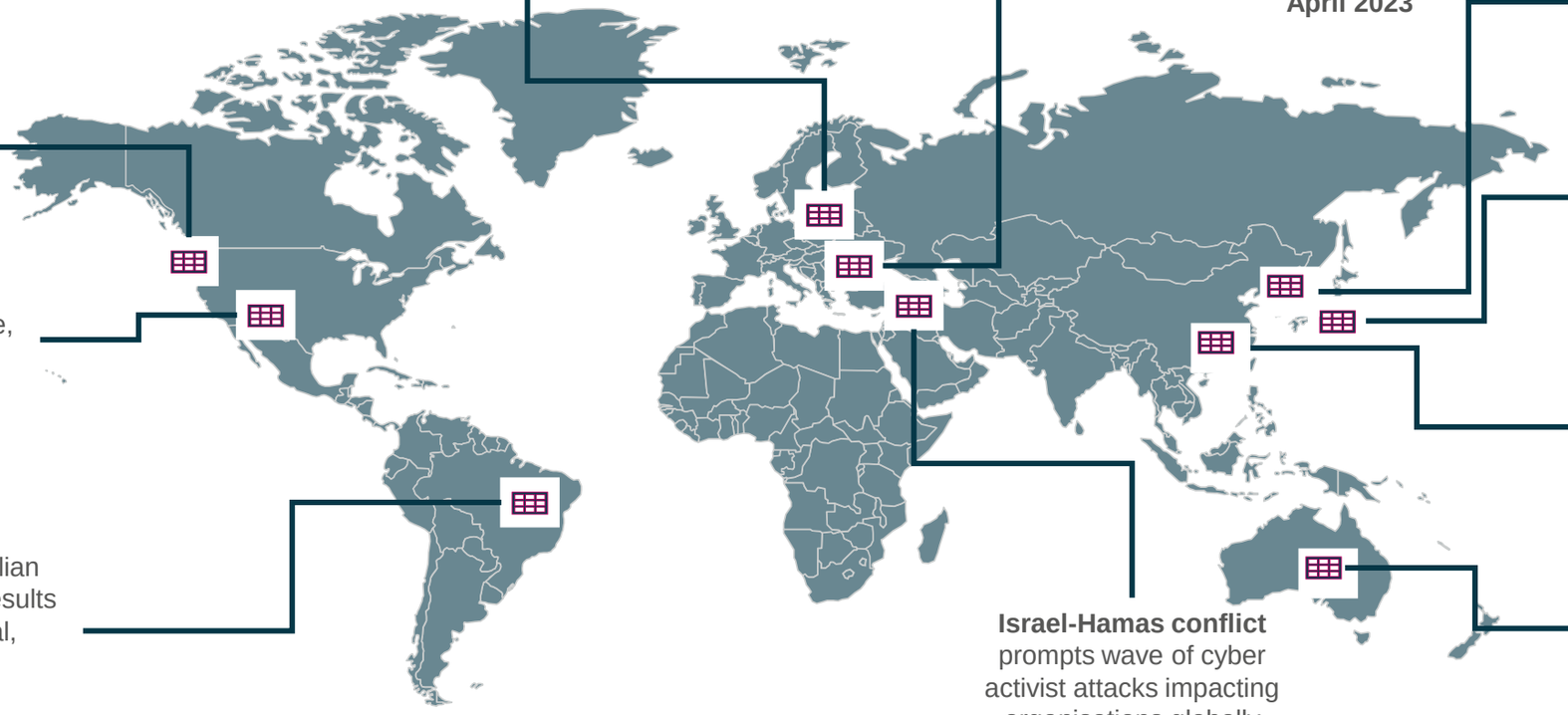
Pentagon Leaks underscores persistent insider threat to defence, government organisations
April 2023

Hong Kong office of UK engineering firm loses USD25m in **deepfake payment diversion fraud**
February 2024

Ransomware attack on Brazilian **construction** conglomerate results in theft of sensitive personal, business data
March 2023

Israel-Hamas conflict prompts wave of cyber activist attacks impacting organisations globally
October 2023

Spate of ransomware attacks, data breaches spurs **regulatory changes** – **September 2023**



Control Risks: Internal database

Digital integrity | Threats to Australia

Ransomware causing up to AUD 3b in damages to the Australian economy per year – December 2023

In 2023, the number of extortion-related cyber incidents that the ASD responded to, increased by 8% compared to the previous year. Over 90% of these involved ransomware. High profile incidents include Medibank, Optus, Medisecure and DP World.

Victoria's government supplier bank details changed in payment diversion fraud – February 2024

The Victorian Auditor General's Office said that supplier payment details held in a master file by the department had been altered four times within 18 months. Threat actors alter such details to re-direct payments to bank accounts held in their name.

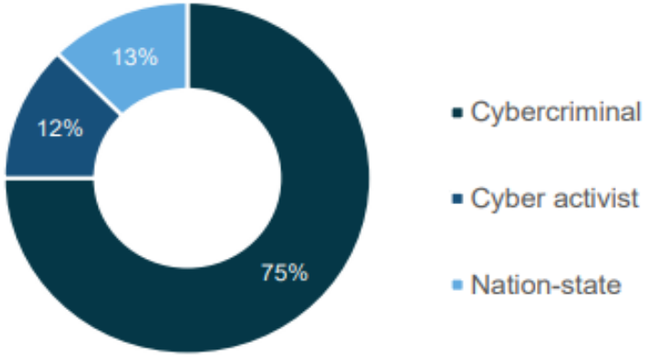
Australian organisations, government entities targeted in espionage campaigns – February 2024

Five Eyes community has warned over China-linked threat group Volt Typhoon conducting reconnaissance on entities to conduct pre-position campaigns.

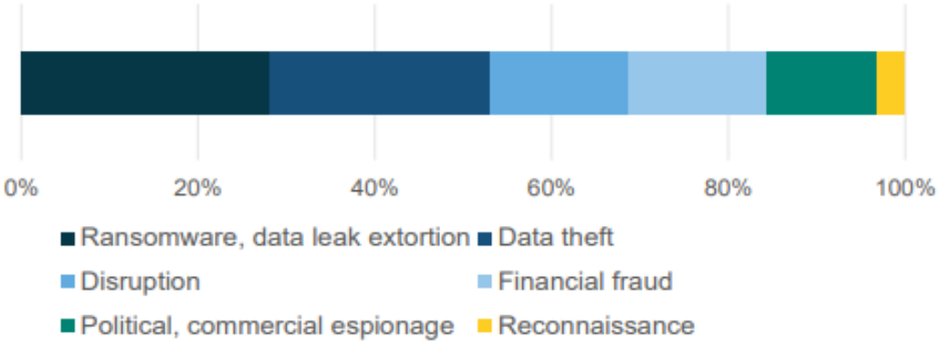
Increasing costs of insider risks highlights growing threats to organisations reliant on contractors – September 2023

Insider threat actors have varying intents to target organisations, however, due to their existing access and knowledge of the companies' networks, they can cause considerable impacts. The threat of insiders is heightened for organisations that frequently work with contractors that have access to their systems.

Share of strategically significant cyber attacks targeting Australia by threat actor (2022-24)



Share of strategically significant attacks targeting Australia by attack type (2022-24)



Control Risks: Internal database

Digital integrity | Current and emerging AI risks

Below are the most immediately relevant threats at an organisational and AI system level.

Longer term **job displacement, social manipulation, dependency and skills loss, bias, fairness, ethical** and **environmental** risks will require combined state, private solutions.

CURRENT

EMERGING

DISINFORMATION & ACTIVISM

Election interference

Strategic disinformation / social manipulation

Targeted campaigns (geopolitical and ideological motives)

AI activism

SOCIAL ENGINEERING

AI-enabled fraud (including deepfakes and deepvoice)

Tailored phishing emails

Social engineering learning and analysis

ATTACKS AGAINST AI SYSTEMS

Confidentiality attacks

Disruptive attacks

Extortive attacks

Evasion attacks

INTEGRITY ATTACKS

Poisoning attacks

Abuse attacks

Model inversion

Model tampering

AI-ENABLED CYBER ATTACKS

AI-enabled reconnaissance and target selection

AI-enabled vulnerability enumeration

AI-enabled cyber resource generation

Significant volume increase

Case studies: Digital integrity | Third party vulnerabilities

What happened?

- Stolen credentials used by a third-party IT service provider
- Accessed Medibank's network through a misconfigured firewall
- Significant extortion attempts and publication of personal data

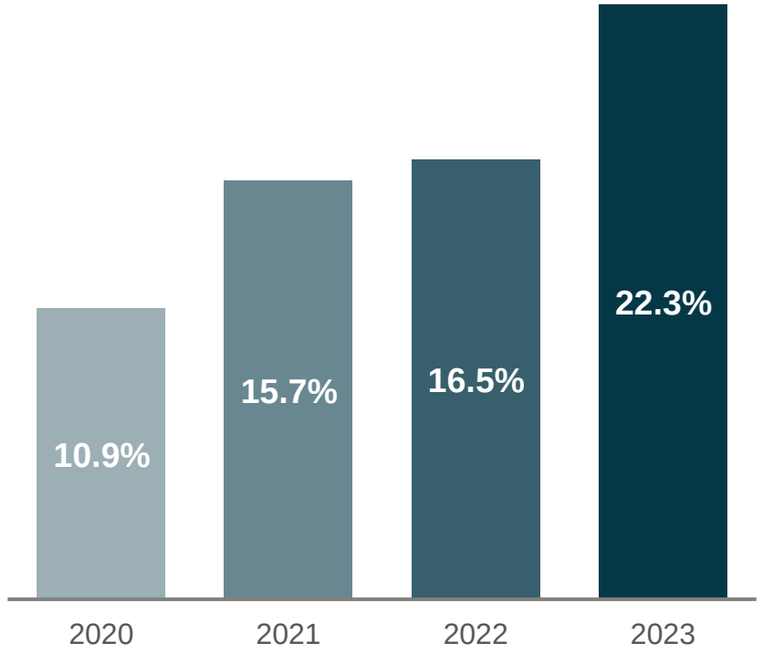
Key learnings (immediate)

- Dynamic subcommittee to liaise with the crisis management team
- Proactive mapping of external parties and retainers in place for rapid support
- Complex communication environment taxed internal capabilities

Key learnings (long term)

- More robust operational risk management - accounting for human error (change management risks)
- Enhanced vetting and focus on critical third parties – risks and controls

Proportion of global cyber incidents impacting third party IT providers (2020-23)



Control Risks: Internal database

Optus Case study: Digital integrity | Third party dependencies

Impact

- ~10 million retail and 400,000 business customers lost network access
- Impact to the economy estimated to be above $2 billion AUD
- 2,696 calls to Triple Zero unable to be connected

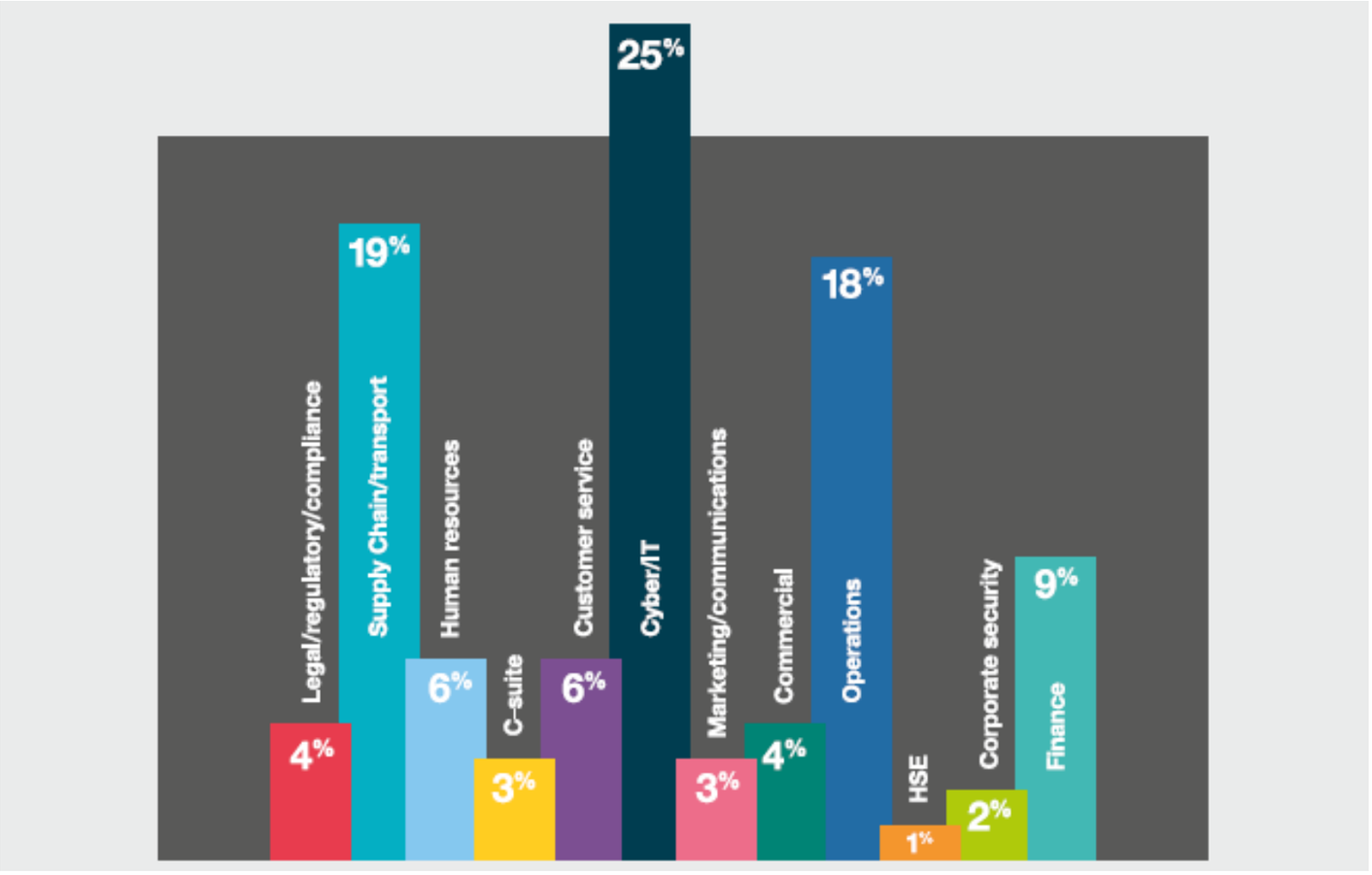
Considerations

- Many organisations did not have alternate communications in place
- Some organisations had recognised the loss of Optus services as a risk, but rated the likelihood as low enough that mitigation hadn't been established

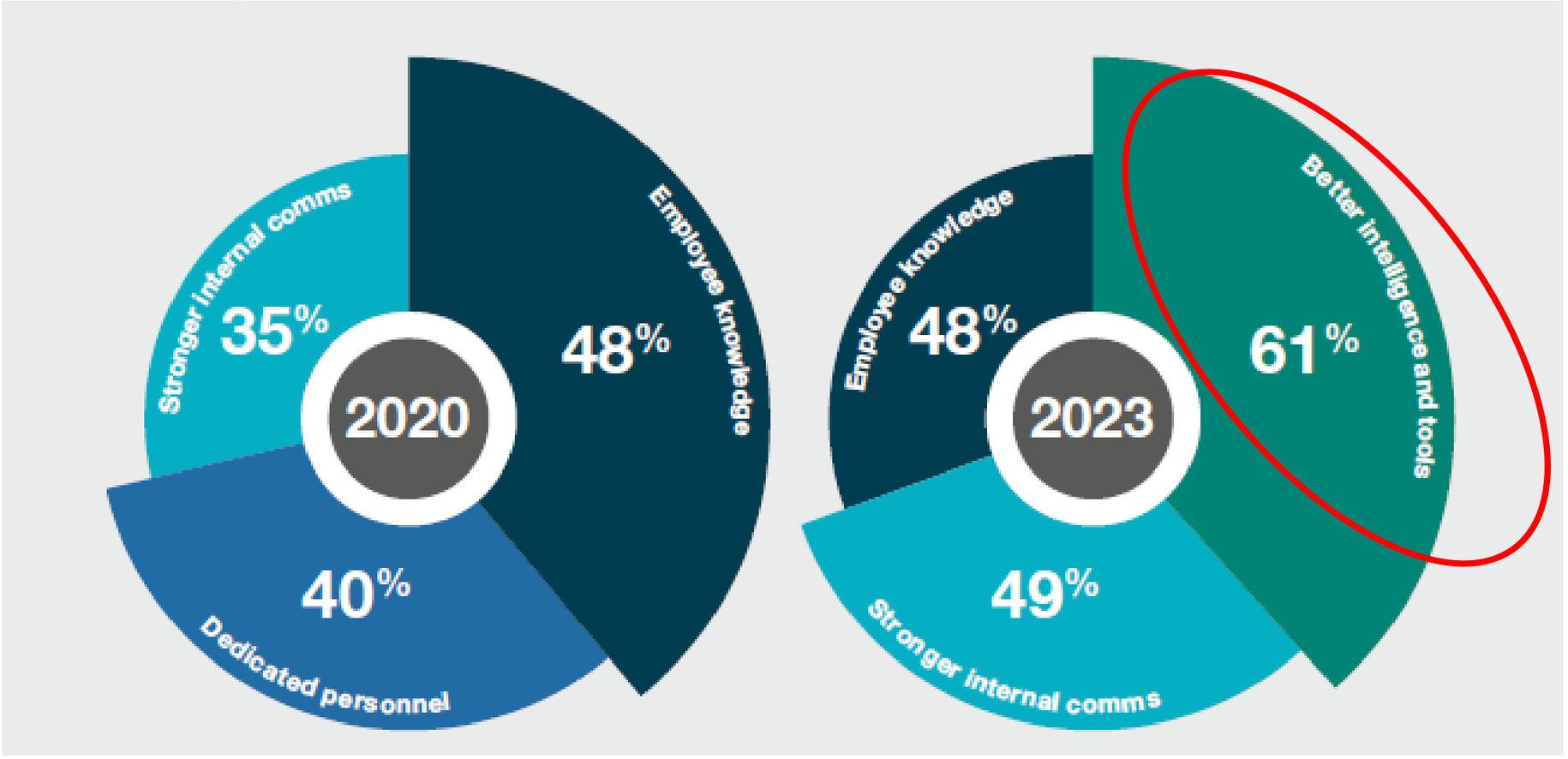
Which organisations succeeded?

- Those who had identified the network as a critical dependency and established mitigation (wireless dongles, redundant networks, pagers)
- Some organisations had further mapped this across critical staff, however others had redundant capability, but only for their offices

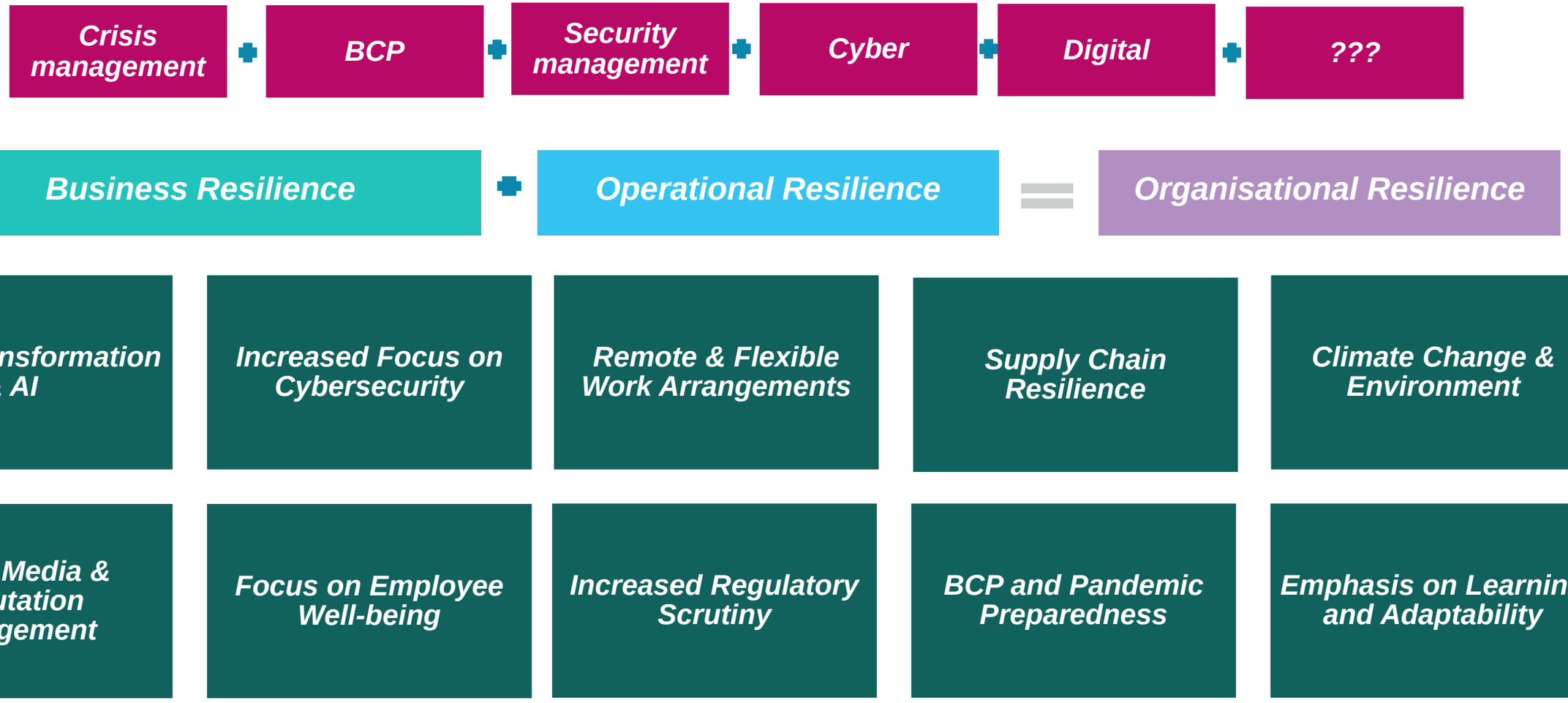
What business function has been most impacted in the past two years?



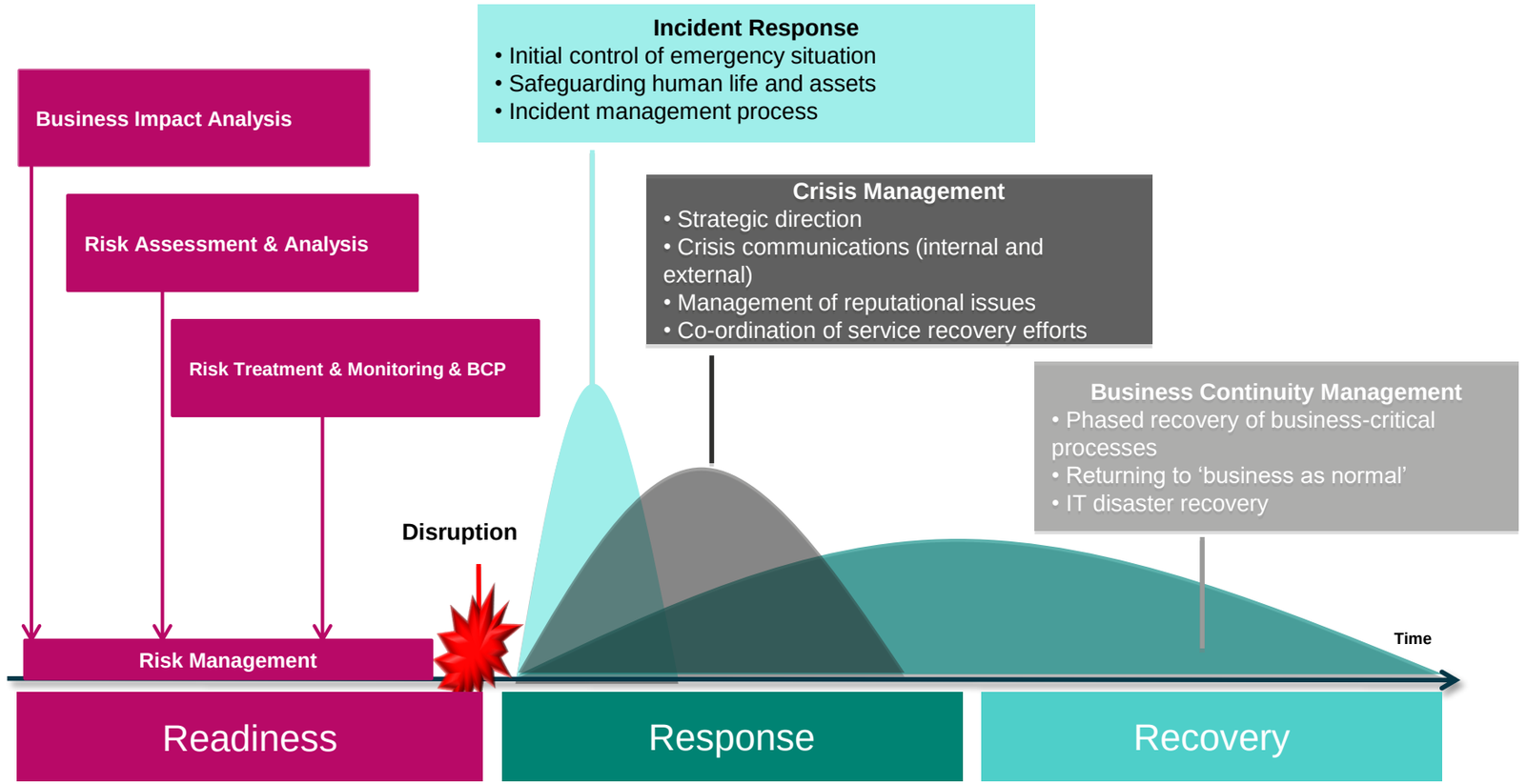
What would strengthen your ability to withstand major disruptive events? (respondents selected up to three, unranked)



Wrap up & how resilience is evolving “the construct”



Strengthening operational resilience through enterprise-wide crisis management and business continuity



- Response priorities and objectives aligning with an organisation's strategic goals
- Strong operational & digital resilience (effective business continuity and risk management) ensures critical operations, enabling leadership to focus on strategic rather than tactical decisions.
- Crisis management is adaptable to various crisis conditions.
- Strong escalation, notification, and decision-making processes.
- Structured crisis management agenda focuses the response.

Crisis readiness, response and recovery (3Rs)

01

Readiness

- Crisis management strategy planning
- Business impacts analysis
- Strategic horizon scanning
- Scenario planning
- Crisis program gap analysis and enhancement
- Crisis organization design, governance and program development
- Business continuity planning
- Risk-specific planning
- Crisis exercising and training

02

Response

- Response strategy development
- Executive decision support
- Response execution support
- Threat monitoring and intelligence collection
- Scenario / options analysis
- Stakeholder management and engagement
- Technical imaging and collection

03

Recovery

- Business recovery guidance and strategy
- Recovery project management support
- Ongoing risk monitoring
- Post-incident reviews
- Quantification of loss
- Lessons learned integration
- Continuous improvement

controlrisks.com