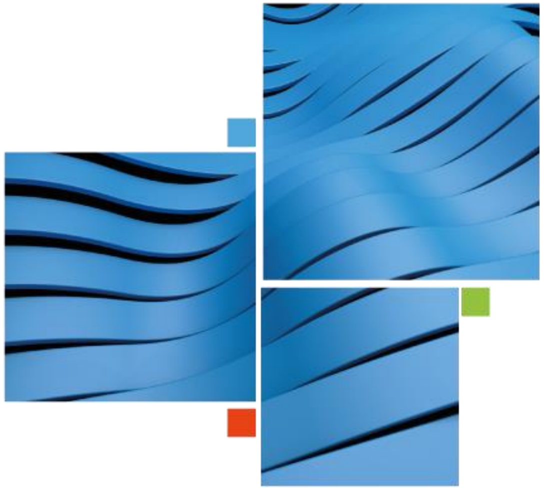
Control Risks

THE STATE OF ENTERPRISE RESILIENCE

Resilience Survey 2016/17

Resilience survey analysis and implications for business



November 2016

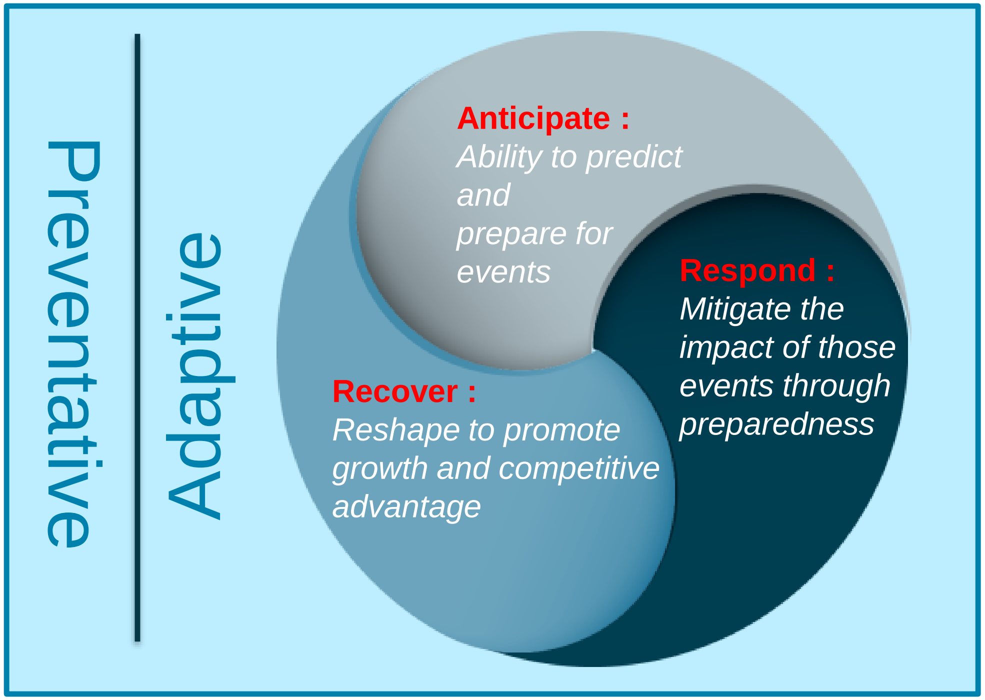
Control Risks

What is resilience?

Resilience is an organisations ability to **assess, anticipate, prepare for and recover from disruptive events** while creating **competitive advantage**.

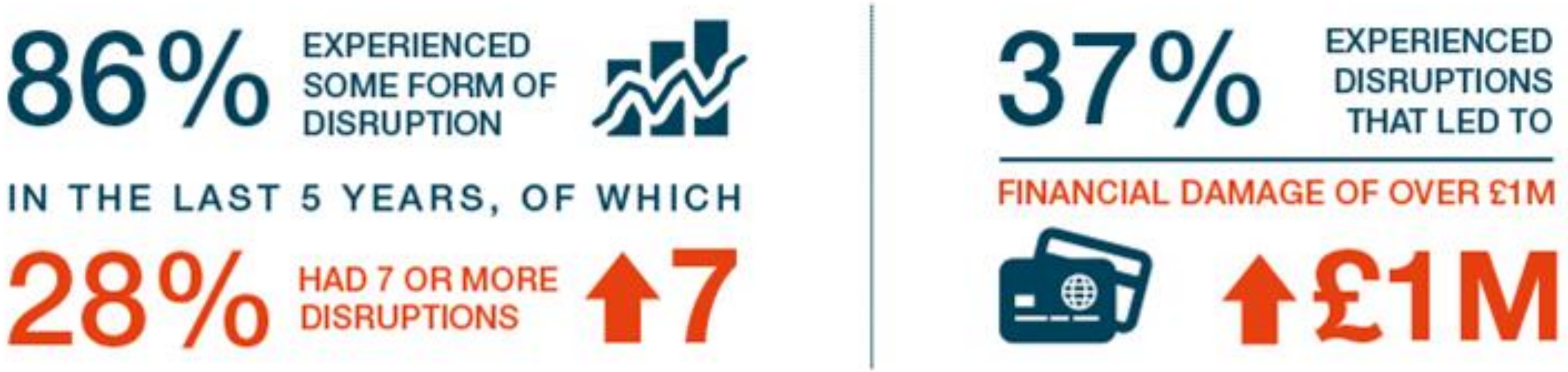
Initially focussed on protection from adverse events that could affect organisational performance.

The concept of resilience has moved on considerably, seeking to **enhance capability** and **capacity** to **exploit opportunity**, while also guarding against threats to business objectives.

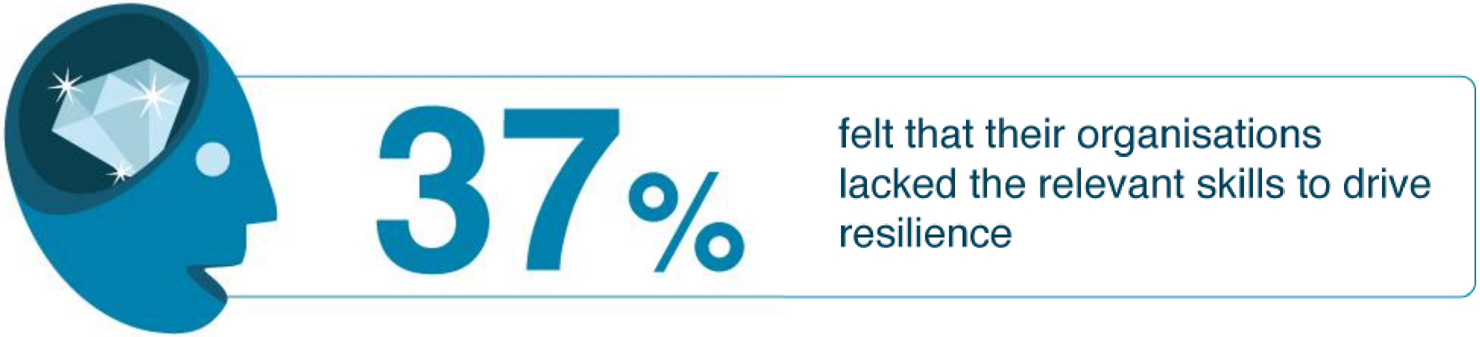

Preventative
Adaptive
Anticipate :
Ability to predict and prepare for events
Respond :
Mitigate the impact of those events through preparedness
Recover :
Reshape to promote growth and competitive advantage

Context: 2015 resilience survey summary

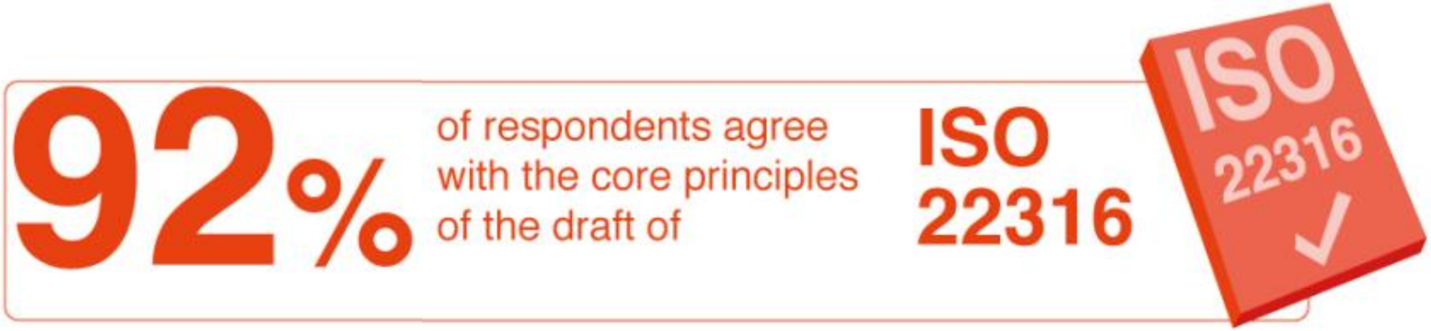
Our global survey found that **52% of respondents** felt that their organisations captured global risk and opportunities well however…


86% EXPERIENCED SOME FORM OF DISRUPTION
IN THE LAST 5 YEARS, OF WHICH
28% HAD 7 OR MORE DISRUPTIONS
7
37% EXPERIENCED DISRUPTIONS THAT LED TO
FINANCIAL DAMAGE OF OVER £1M
£1M

2016 Survey: key findings



37% felt that their organisations lacked the relevant skills to drive resilience



92% of respondents agree with the core principles of the draft of ISO 22316

2016 Survey: key findings

47%

state that **cyber threat** is a primary concern

92%

agree that **cross-functional working** and **sharing of information** is a **key principle of resilience**

However,

48%

remain **reliant on centralised governance** and oversight

70%

of respondents see **reputational damage** as the impact of most concern

Control Risks

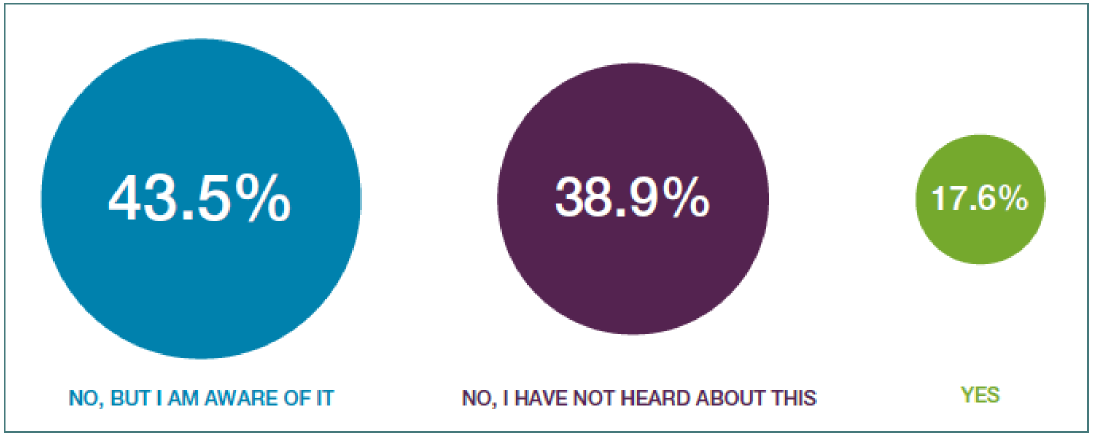
Survey Insights

The challenge of moving from guidance to implementation

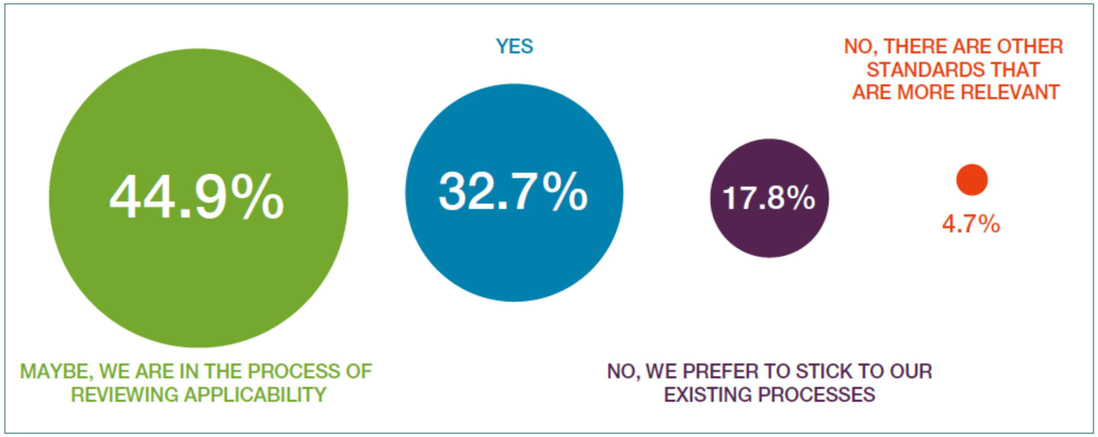
92%

of respondents agree with the core principles of the draft of

ISO 22316



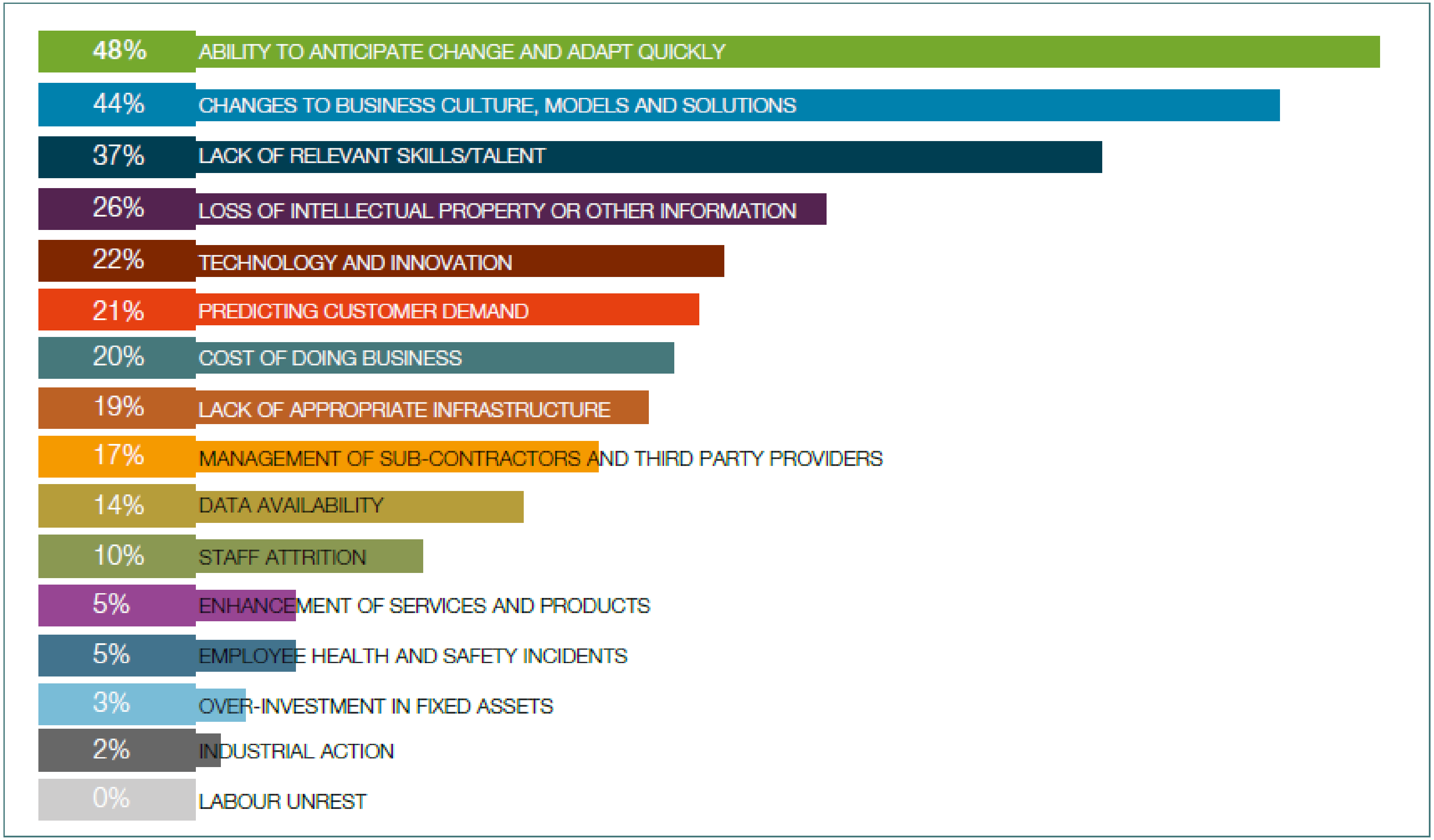
▲ Have you read the draft 'International Standard on Security and Resilience — Guidelines for Organisational Resilience (ISO 22316)'?



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

Control Risks

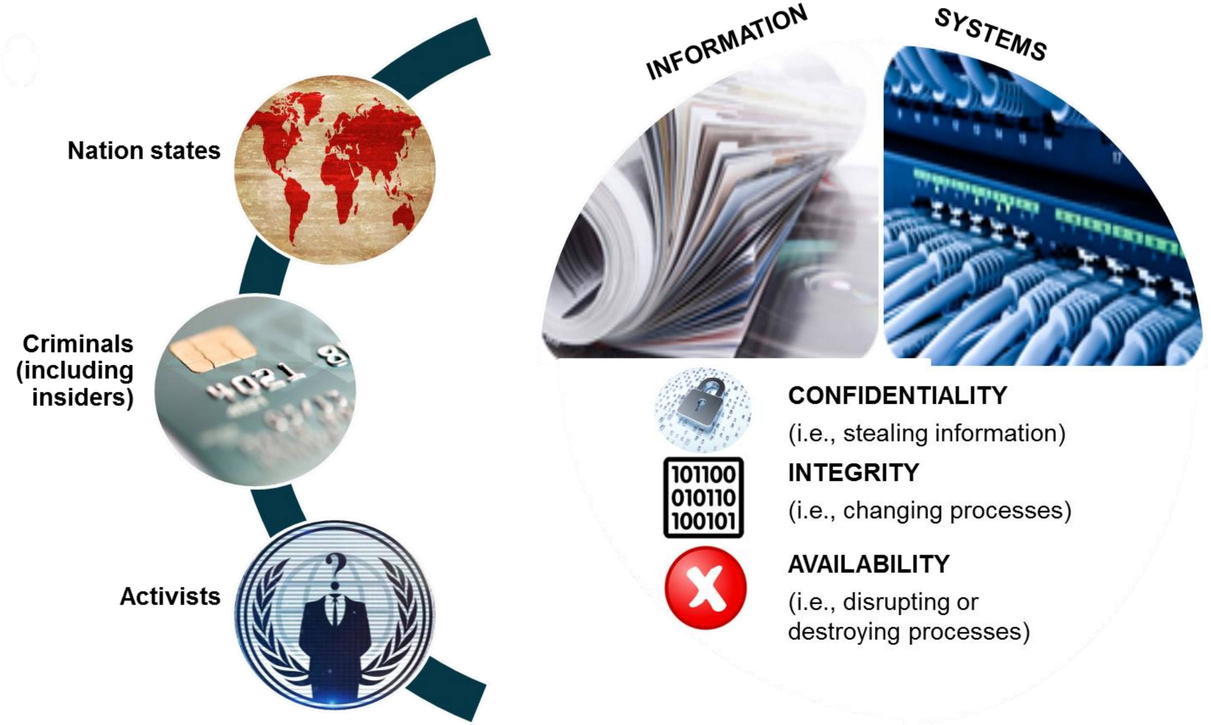
Lack of skills is slowing the implementation down



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

Increasing concern over the cyber threat

47% **State that cyber threat is a primary concern**



Nation states

Criminals (including insiders)

Activists

INFORMATION

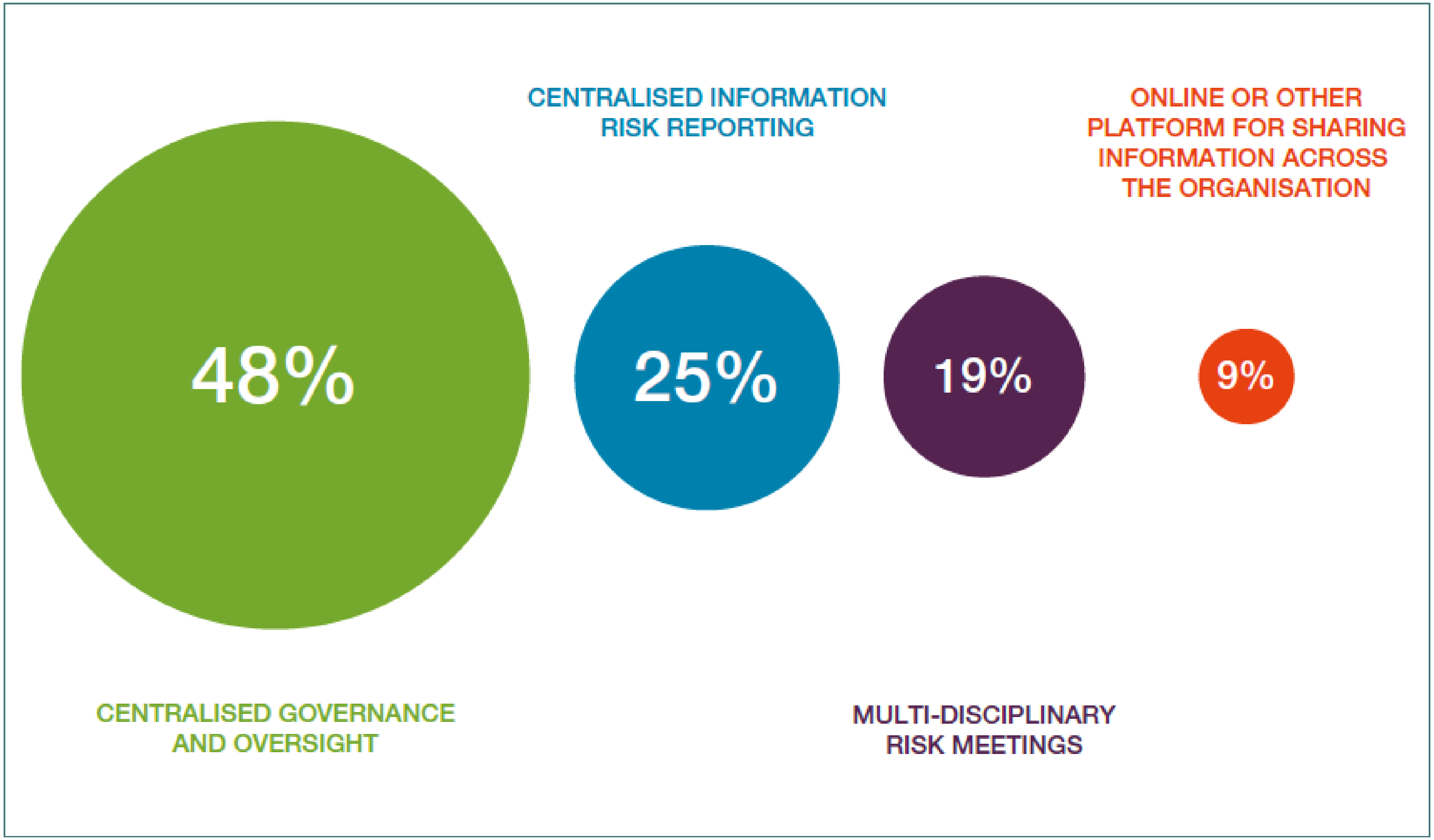
SYSTEMS

CONFIDENTIALITY
(i.e., stealing information)

INTEGRITY
(i.e., changing processes)

AVAILABILITY
(i.e., disrupting or destroying processes)

Reliance on centralised governance and oversight

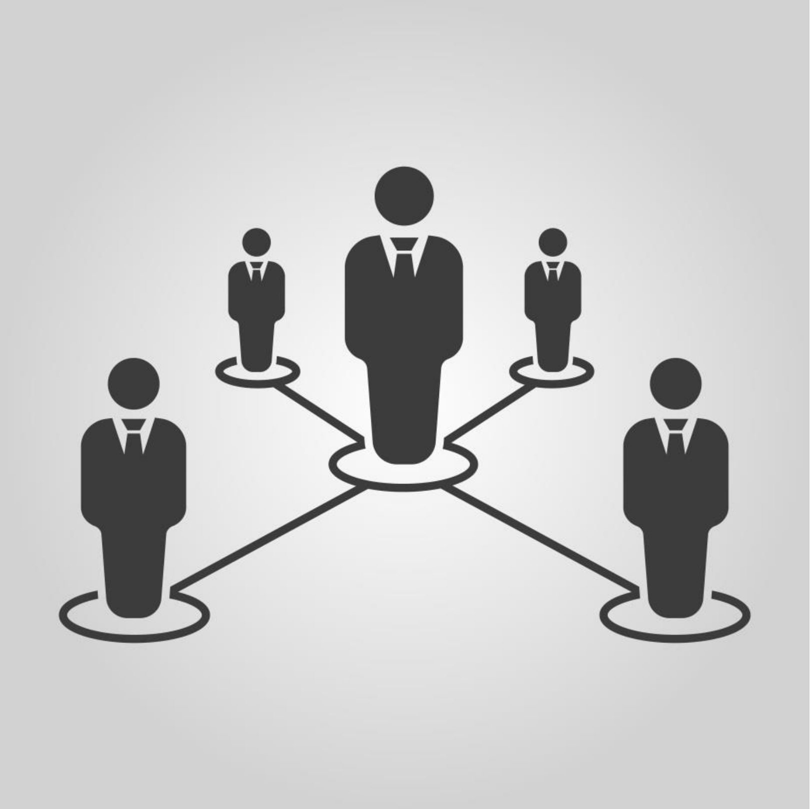


▲ What does your organisation do to encourage resilience management disciplines (strategic planning, financial planning, risk management, business continuity management, crisis management and security management) to work cross functionally?

The importance of effective leadership

53%

"Companies address the challenge of resilience in different ways, but there was unanimous agreement on the fact that **responsibility for resilience should be driven from the executive**."



Recommendations

Recommendations: Build capability

Build the capability of personnel with the essential skills to be able to:

- **Build strong relationships** with stakeholders based on a culture of openness and trust.
- Align interested parties aspirations and objectives with those of the organization to create a **unified commitment to organizational objectives**

- **Reinforce and reward behaviours** that support the organization's vision and core values
- **Translate the strategic approach** to resilience to what is required operationally
- **Empower personnel** to openly communicate about threats and opportunities and initiate problem solving before circumstances escalate

Recommendations: Cyber Risk Management

Four guiding principles:

- Start with the threat
  you cant defend everything
- Combine Social with Technical
  it’s a peoples game
- Have an attacker not a compliance mind-set
  compliance is a baseline only
- Be ready to respond
  attacks are inevitable

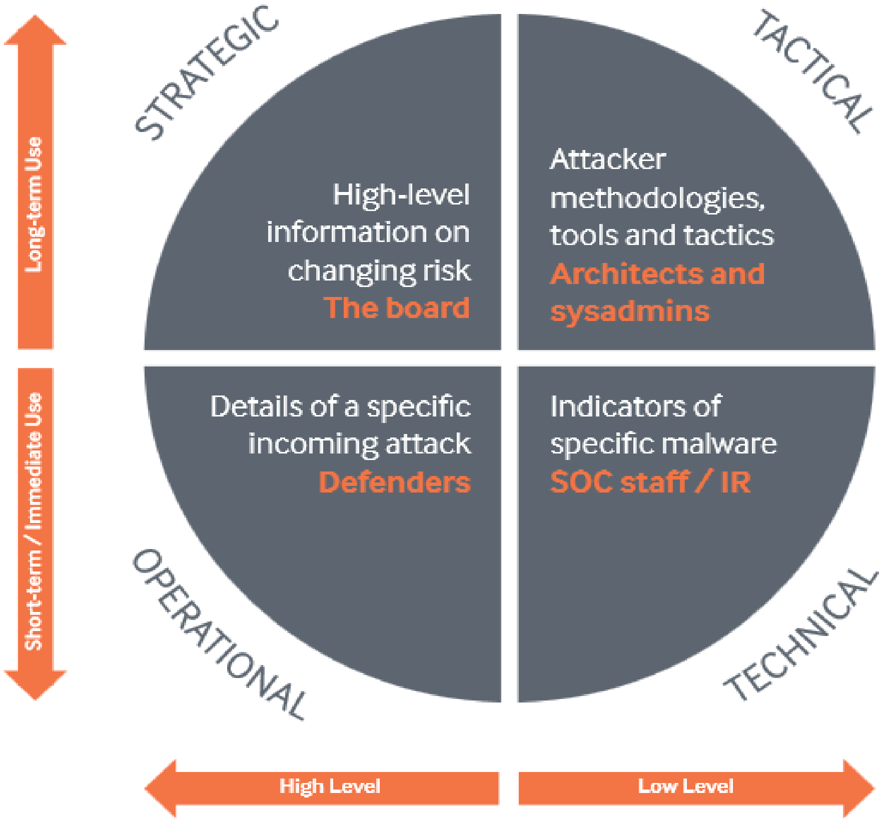
Cyber Protect:
Develop cyber defenses

Cyber Respond:
Immediate breach response

Threat Intelligence:
Understand the threat

Control Risks

Recommendations: Cyber Threat Intelligence



STRATEGIC
TACTICAL
Long-term Use
High-level information on changing risk
The board
Attacker methodologies, tools and tactics
Architects and sysadmins
Short-term / Immediate Use
Details of a specific incoming attack
Defenders
Indicators of specific malware
SOC staff / IR
OPERATIONAL
TECHNICAL
High Level
Low Level

Source: CERT-UK and Centre for Protection of National Infrastructure sponsored paper, by MWR InfoSecurity

Control Risks

Recommendations: TOP 8 questions to ask your Board, Executive and Leadership team

1. Do you know who is **targeting** your information and assets?
2. Do you know how you might be attacked?
3. Do you know which assets, if breached, would be most **business critical?**
4. Do you have **a response plan** in the event of a major breach?
5. Do you have a **dedicated owner for cyber & information security risk?**
6. Have you **rehearsed** your response to the most likely scenarios?
7. Is your Board **cyber risk aware** and **prepared?**
8. Do you understand your **third party cyber risk?**

Recommendations: Integrated Risk Management

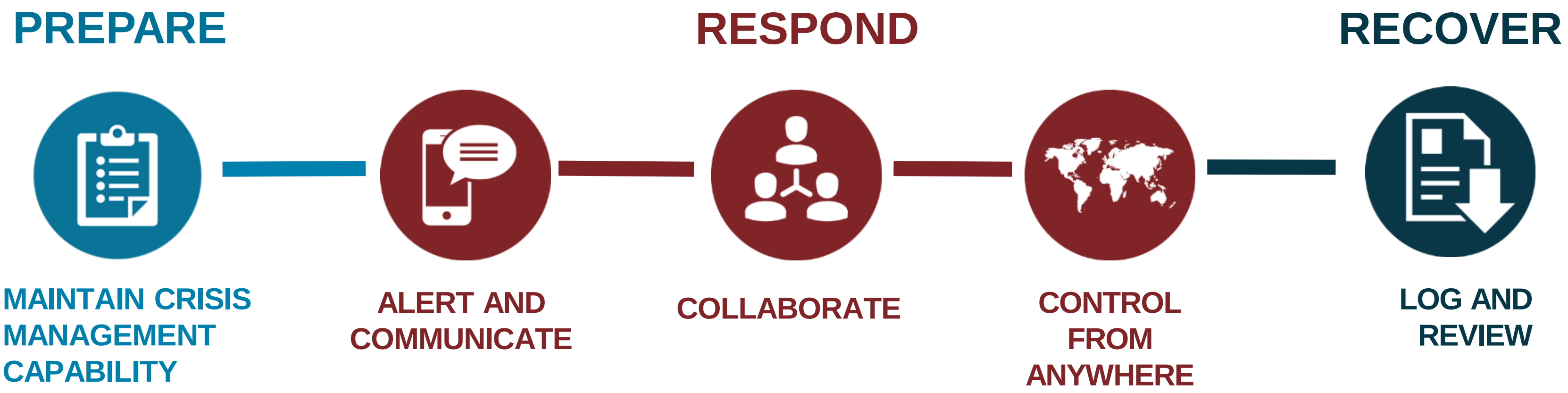
Integrate the risk management activities and operational disciplines, thereby ensuring that knowledge is actively shared across internal organisational boundaries.

Control Risks repeatedly being asked to recommend tools for:

- Accounting for people and mass communications platforms with geo-location of incidents and affected/unaffected parties.
- Incident management including; communications, all informed participation providing "single source of truth", collaborative working, logging and recording.
- Tools to enable CM teams to concentrate on strategic decisions and not spend valuable time enacting administrative processes.

Control Risks

Integrated Risk Management


PREPARE

RESPOND

RECOVER

MAINTAIN CRISIS MANAGEMENT CAPABILITY

ALERT AND COMMUNICATE

COLLABORATE

CONTROL FROM ANYWHERE

LOG AND REVIEW

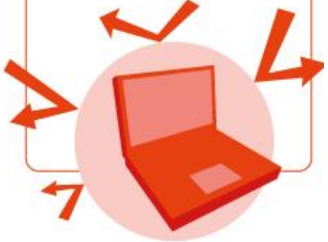
Conclusion

Key findings

37% felt that their organisations lacked the relevant skills to drive resilience

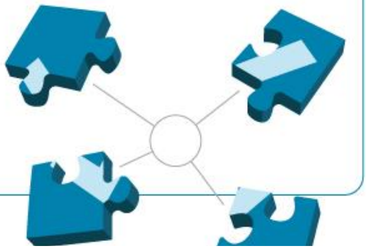
92% of respondents agree with the core principles of the draft of **ISO 22316**

47% state that **cyber threat** is a primary concern



92% agree that **cross-functional working** and **sharing of information** is a **key principle of resilience**

However, **48%** remain **reliant on centralised governance** and oversight



70% of respondents see **reputational damage** as the impact of most concern

Andy Cox, Director
andy.cox@controlrisks.com