bsi.

bci Thought Leadership

BCI Horizon Scan Report 2022

BNZBA

www.thebci.org

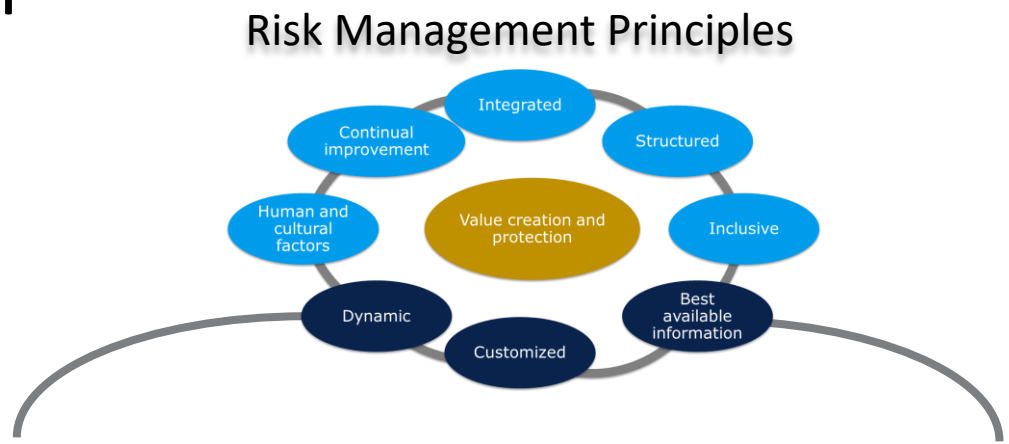
bci Leading the way to resilience

PROFILE: SIMON JORDAN

- Bachelor of Sciences (Earth Sciences) – Waikato University 1997
- Member of the Business Continuity Institute
- ISO22031/ISO27001 Lead Implementer, IRCA Certified ISO27001 Information Security Lead Auditor
- Over 20 years of business experience in both NZ and the UK
- Business/technical mix covering Business Continuity, Disaster Recovery, Information Security, Risk, Information Technology and Networking and Business
- BSI External Trainer – Business Continuity, Information Security, Risk and Asset Management Systems
- 2019 BCI Australasian Business Continuity and Resilience Consultant of the Year, BCI Global Finalist

Company	Role	Responsibilities
Resilient IT	Managing Director/Principal Consultant - Auckland	*Business Continuity, Information Security and Risk Consulting*
Plan B	Key Account Manager – Wellington/Auckland	*Top 35 Accounts - Insurance, Banking, Retail, Legal, Logistics, Distribution*
IBM	Key Accounts - Systems & Technology - Wellington	*BNZ, ANZ, MoH, Police, Customs, Southern DHB's, NIWA*
Gen-i/Spark	Business Solutions Specialist - Wellington	*Infrastructure and WAN specialist - Enterprise and Government*
Itegrity (UK)	Director/Security Specialist - London	*Banking, Legal and Government*
ComputerLand	Account Manager - Hamilton	*Corporate Accounts & Education Sector*

Introduction



Dynamic

Risks can emerge, change or disappear as an organization's external and internal context changes. Risk management **anticipates**, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.

Best available information

The inputs to risk management are based on historical and current information, as well as on **future expectations**. Risk management explicitly takes into account imitations and **uncertainties** associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders

Context

Source: ISO31000:2018

Leading the way to resilience

bsi.

About the Horizon Scan 2022 Report

Leading the way to resilience

Risk and Threat Assessment: Last Twelve Months

www.thebci.org

bci Leading the way to resilience

Risk and threat assessment: past twelve months

Rank	Event	Frequency	Impact	Risk Index
1	Non-occupational disease (e.g. pandemic)	9.7	2.5	24.5
2	(Issues arising from) remote working/new workplace environment	11.4	2.1	24.3
3	Travel restrictions	10.0	2.1	21.5
4	Health incident (NOT transmissible disease such as COVID but occupational disease, reportable occupational disease, stress/mental health, increased sickness absence)	9.4	1.9	17.9
5	Lack of talent/key skills	8.0	2.2	17.3
6	Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident)	7.8	1.9	14.5
7	Supply chain disruption	6.3	2.1	13.3
8	IT and telecom outage	6.1	2.0	12.3
9	Cyber attack & data breach	6.0	2.0	11.7
10	Lone attacker/active shooter incident	4.8	2.3	11.1
11	Extreme weather events (e.g. floods, storms, freeze, etc.)	5.4	2.0	10.9
12	Regulatory changes	5.2	2.1	10.9
13	Natural resources shortage	5.2	2.0	10.3
14	Higher cost of borrowing	5.4	1.9	10.2
15	Interruption to utility supply	5.0	1.9	9.7
16	Exchange rate volatility	4.8	2.0	9.6

Risk and threat assessment: pa

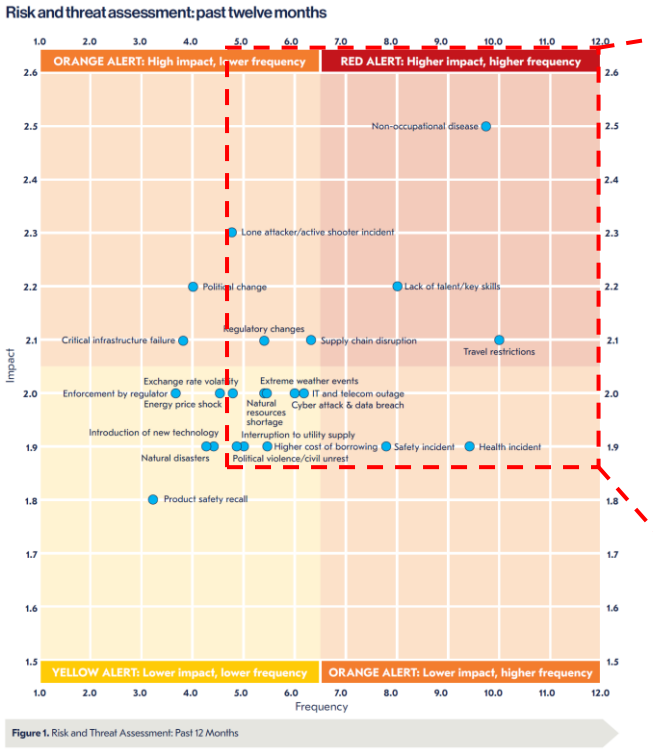
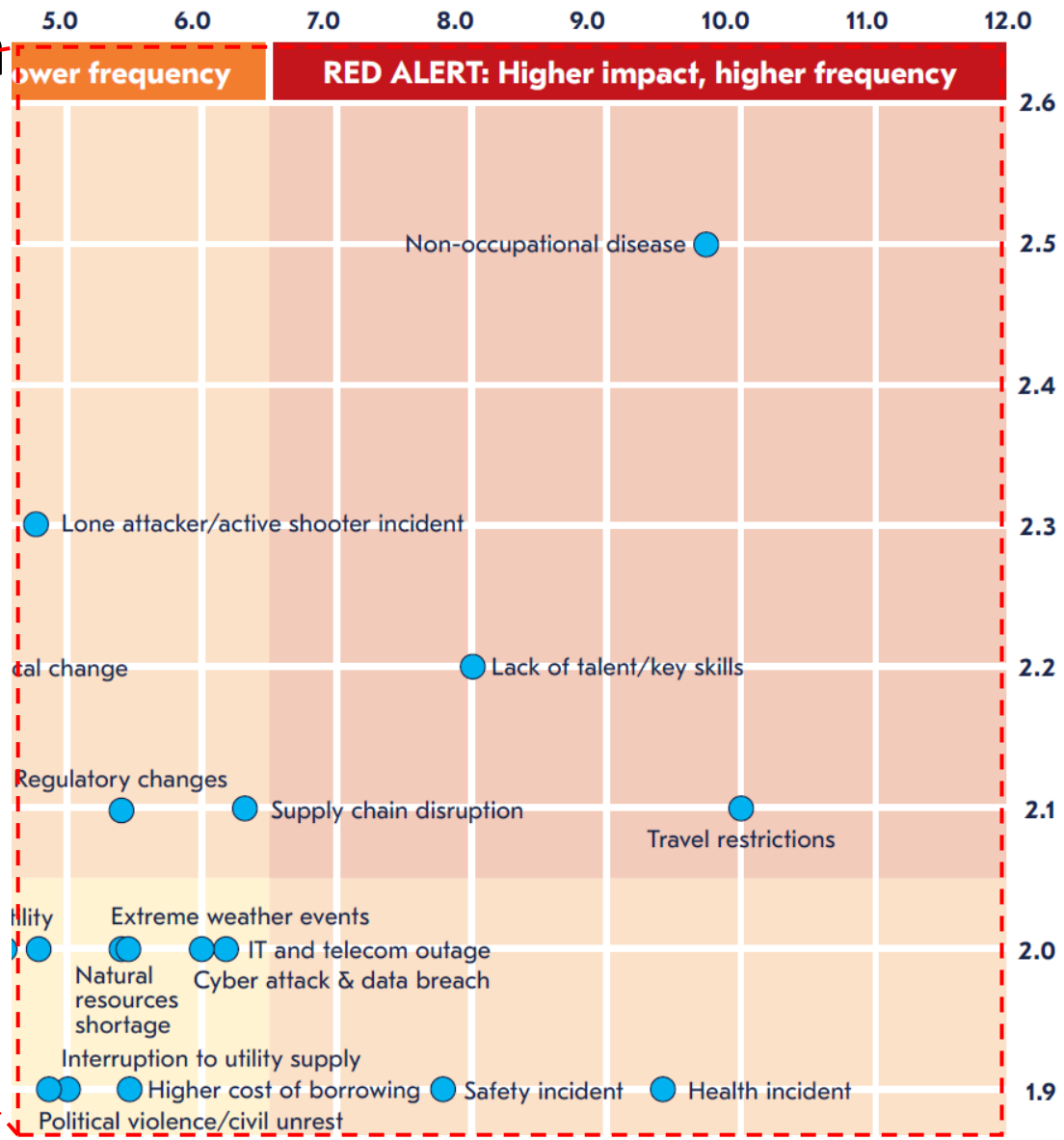
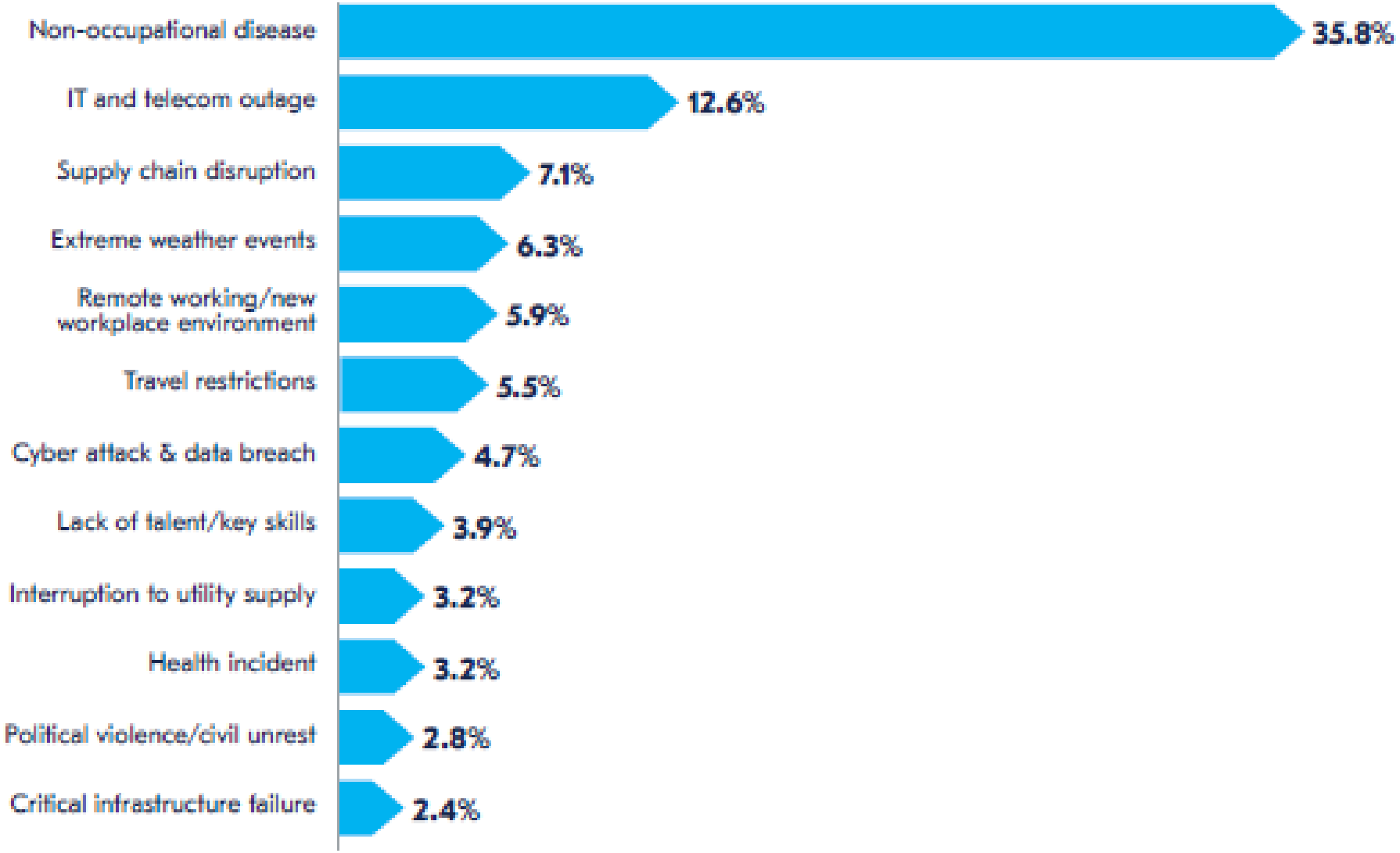


Figure 1. Risk and Threat Assessment: Past 12 Months



Which of the above events the most major disruption in the past year?



Leading the way to resilience

bsi.

Risk and Threat Assessment: Next Twelve Months

www.thebci.org

Risk and threat assessment: next twelve months

- The pandemic remains top of organisations' concerns for 2022 – but is this still now the case with increasing global tensions?
- Cyber security strategies will be tested in 2022, with attacks now targeted towards global supply chains.
- IT and telecoms outages remain at the top of the list and, with organisations becoming increasingly dependent on a single platform for all communications, there is concern that many do not have sufficient back-up processes in place.
- Severe weather continues to be a concern, although most organisations have yet to consider the chronic threat of climate change in their planning strategies.

Risk and threat assessment: next twelve months

Rank	Event	Likelihood	Impact	Risk score
1	Non-occupational disease	3.9	2	7.8
2	Cyber attack & data breach	3.1	2.2	6.9
3	Travel restrictions	3.5	1.6	5.6
4	(Issues arising from) remote working/new workplace environment	3.6	1.4	5.0
5	IT and telecom outage	2.9	1.7	4.9
6	Extreme weather events (e.g. floods, storms, freeze, etc.)	3	1.6	4.8
7	Critical infrastructure failure	2.4	2	4.8
8	Regulatory changes	2.8	1.7	4.8
9	Lack of talent/key skills	2.6	1.8	4.7
10	Health incident (NOT transmissible disease such as COVID but occupational disease, reportable occupational disease, stress/mental health, increased sickness absence)	2.8	1.6	4.5
11	Supply chain disruption	2.5	1.7	4.3
12	Introduction of new technology (IoT, AI, Big data)	2.7	1.5	4.1
13	Natural disasters (earthquakes, tsunamis, etc.)	2.1	1.9	4.0
14	Safety incident (personal injury, fatality, asset damage, dangerous occurrence, reportable incident)	2.4	1.6	3.8
15	Lone attacker/active shooter incident	1.8	2.1	3.8

Risk and threat assessment: past twelve months

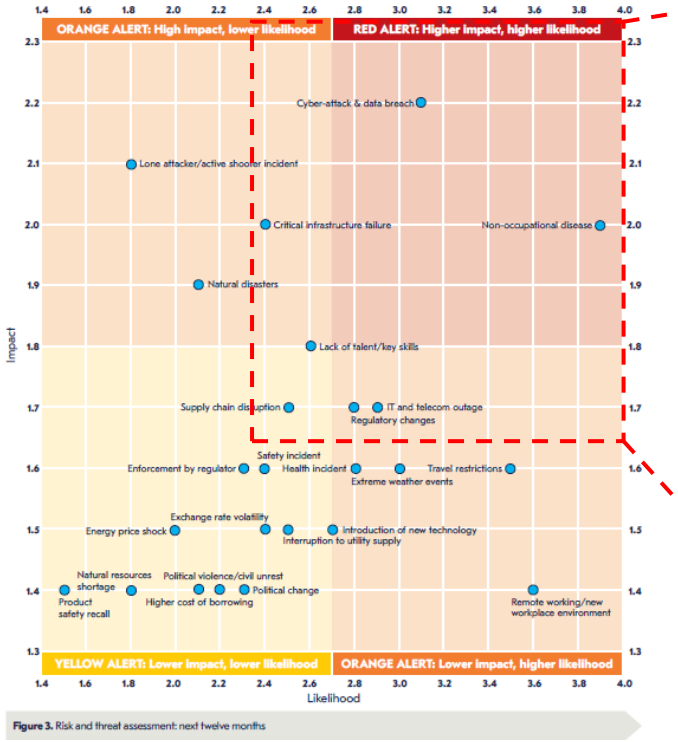
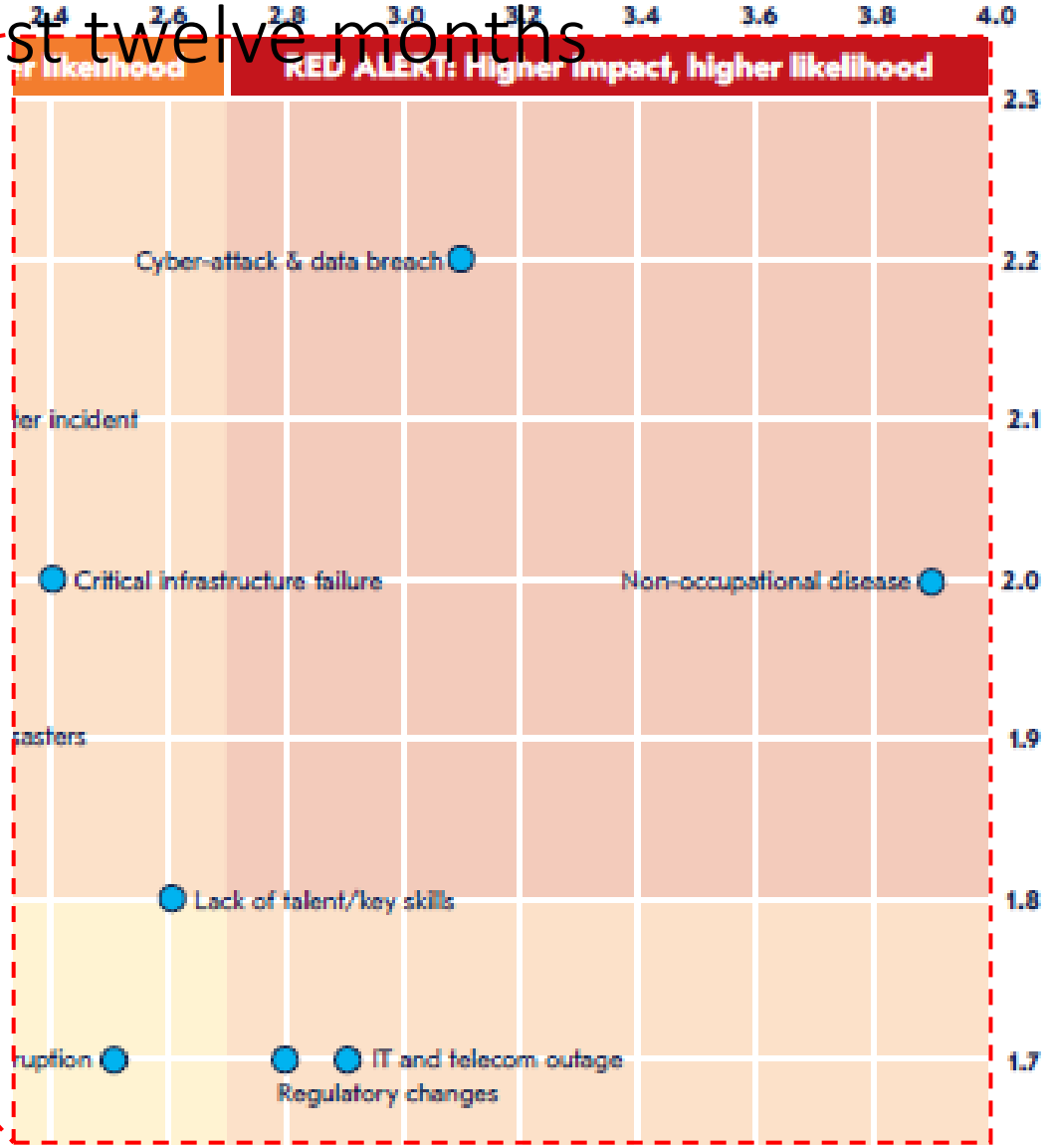


Figure 3. Risk and threat assessment: next twelve months



Leading the way to resilience

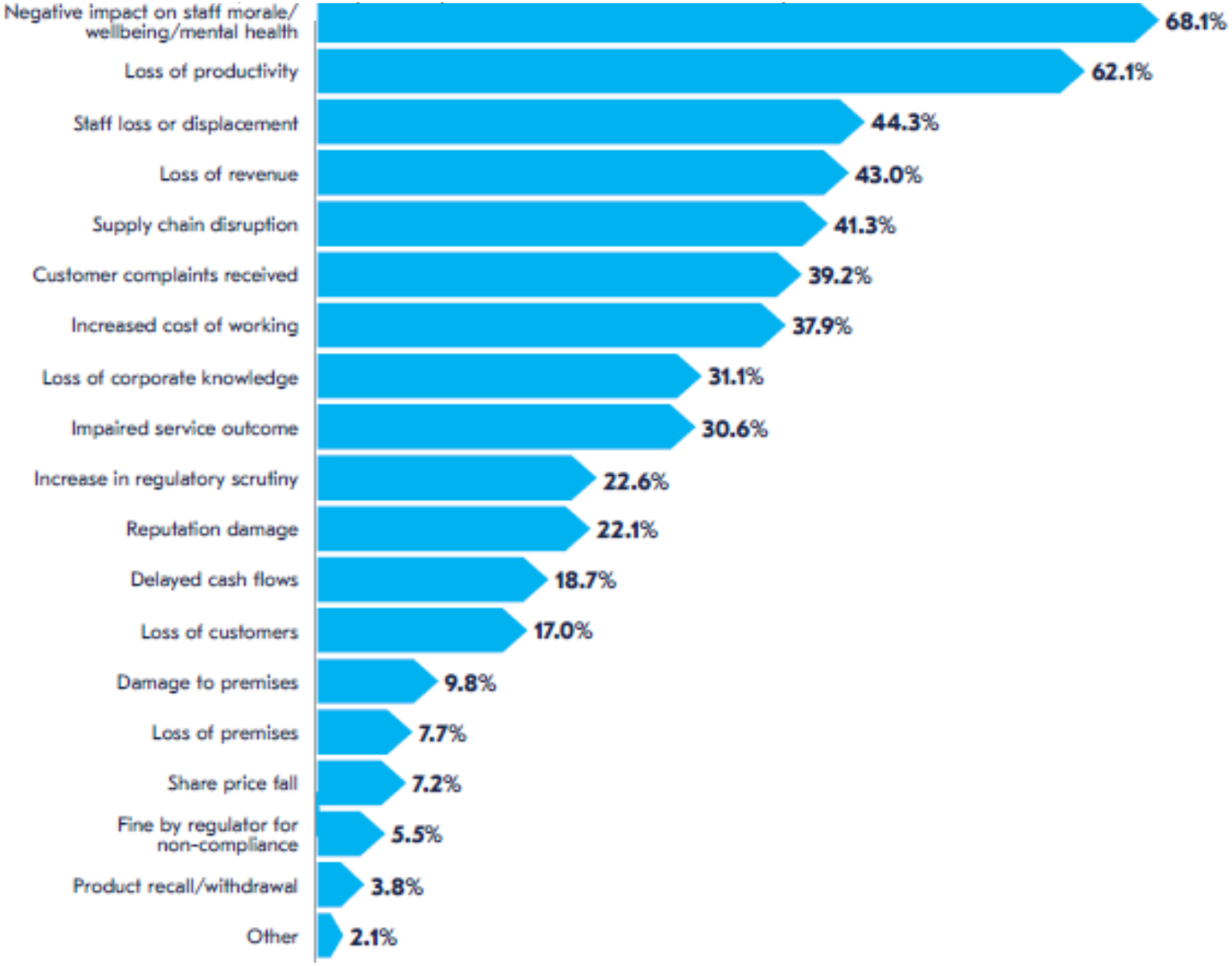
bsi.

Consequences of Disruptions

Consequences of Disruption

- **Staff morale**, **wellbeing** and **mental health** is now the greatest consequence of disruption for organisations demonstrating the increased focus on staff wellbeing programmes exhibited in the early stages of the pandemic needs to continue.
- **Staff loss** or **displacement** was reported as a **major concern** by nearly half of respondents showing that the **‘great resignation’** is a reality for many organisations.
- **Excuses** of COVID-19 as a cause for poor customer service or product/service delays is now **wearing thin**. Respondents reported rises in customer complaints and reputational damage over the past year demonstrating customers are becoming **less forgiving** of bad service.

Impacts or consequences that arose from the disruptions exp



bci Leading the way to resilience

bsi.

Benchmarking Business Continuity

www.thebci.org

Business Continuity Benchmarks

- ISO 22301 remains the business continuity benchmark for nine out of ten organizations.
- Although certification levels fell slightly during 2021, the number of organizations using ISO 22301 as a framework increased by 11 percentage points over the year.

Top 10 standards used within organizations (aside from ISO 22301)		
1	ISO 27001	Information security management
2	ISO 31000	Risk Management
3	ISO 9001	Quality
4	ISO 22316	Organizational Resilience
5	NIST Framework	Information Security
6	COSO Framework	Internal Control
7	ISO 45001	Health and Safety
8	ISO 14001	Environmental Management
9	ISO 22320	Incident Response
10	COBIT	Information Technology

bci Leading the way to resilience

bsi.

Benchmarking longer term trend analysis

- In the mid- to long-term, **cyber-security** was cited as a top concern by 85% of practitioners.
- Climate risk is an **emerging risk**, with worsening extreme weather and elevated concerns arising from COP26 encouraging practitioners to consider how climate change will affect their organization in the long term (chronic) rather than short term (acute).
- Less than half of organisations have centralised their risk scanning processes, with many labelling it as an ‘area cited for improvement’ during 2022.

In the next 5-10 years, top three concerns for the mid- to long-term r

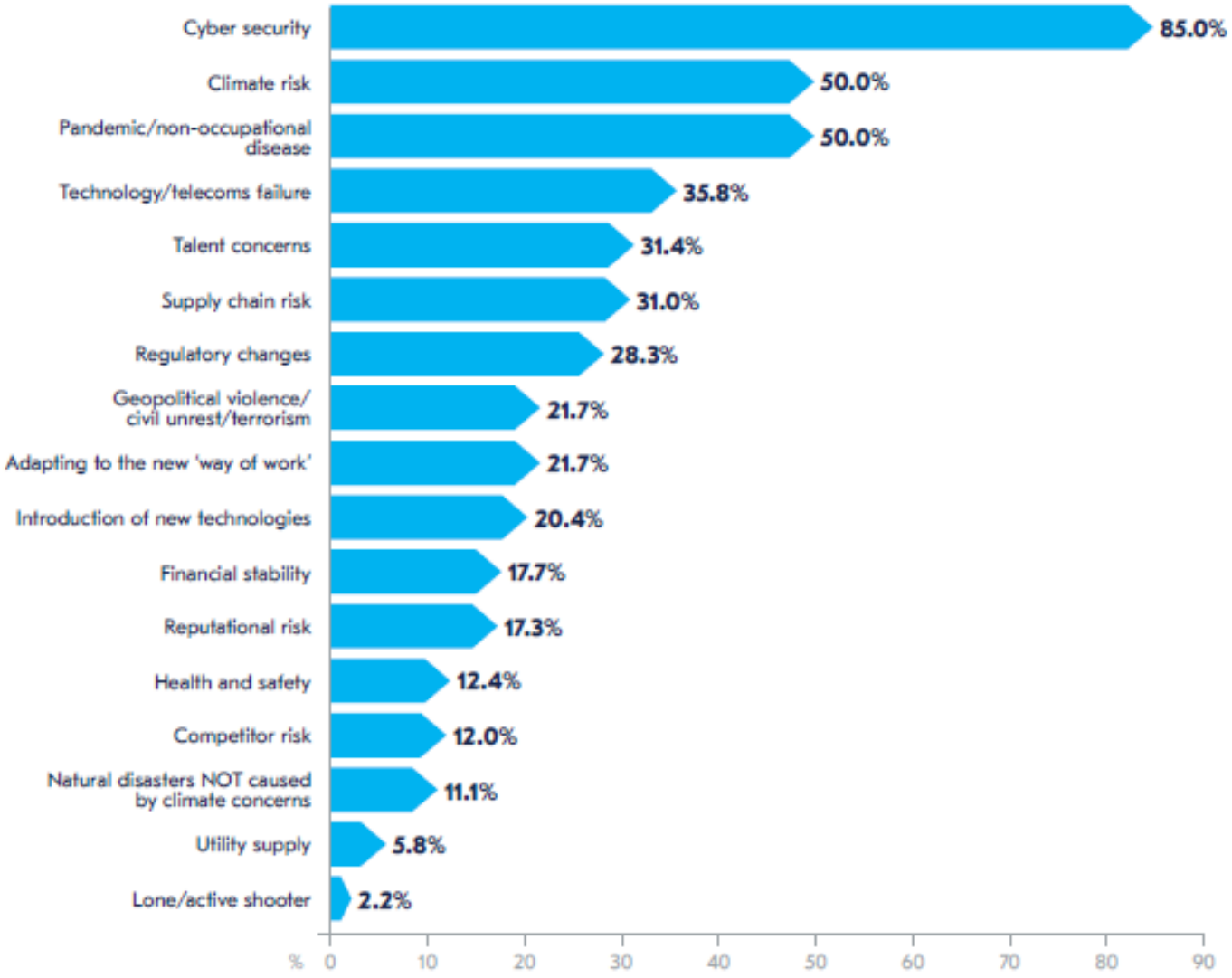


Figure 9. Thinking about the next 5-10 years, which are your top three concerns for the mid- to long-term risks?

Benchmarking longer term trend analysis

"Attackers are now taking more of a **spearphishing** approach to target individuals. So the old school phish from a foreign Prince is now dying as everyone is more educated with them, we're seeing a lot more social engineering and targeted phishes. They'll look at your LinkedIn account. They'll look at your social media account. They'll make a speculative intervention with you. At no point will malicious links be shared or anything like that. But they'll build up that knowledge base or the individual. They'll build up that trust, and then deliver the payload when consistent communications and trust is achieved."

Resilience Professional, Utilities, United Kingdom

In Summary

Hybrid workplace environments are testing organizations. Risks such as health and safety concerns, mental health issues and ensuring homeworkers' remote environments are as resilient as those in the office.

Non occupational disease remains the primary perceived threat to organizations and their staff. Natural Risks such as possibility of new viruses, extreme weather are now greater possibilities we need to address. With agreement that climate change will be one of the greatest threats in the next five years.

Cyber threats increased during the pandemic – and are now on a steep rise again and ranked second after non-occupational disease. Criminals are increasingly exploiting homeworkers through social engineering and targeting hastily constructed or networks that lacked security, with attacks causing more devastation for some organizations than ever noted previously.

Supply chain disruptions are also on the rise, as the global shortage for several types of products and services continues. These threats can arise from challenges, such as human resource management, biological and environmental risks, civil unrest or cyber resilience issues. In March, Toyota halted production due to a cyberattack on a critical supplier.

The importance of resilience and business continuity management is being better understood by management in organizations and leading to improved relationships between resilience-orientated

WHAT IS INFORMATION SECURITY?

Information Security is defined as:

"The preservation of confidentiality, integrity and availability of information"

1

Confidentiality

"The property that information is not made available or disclosed to unauthorised individuals, entities or processes"

2

Integrity

"The property of safeguarding the accuracy and completeness of assets"

3

Availability

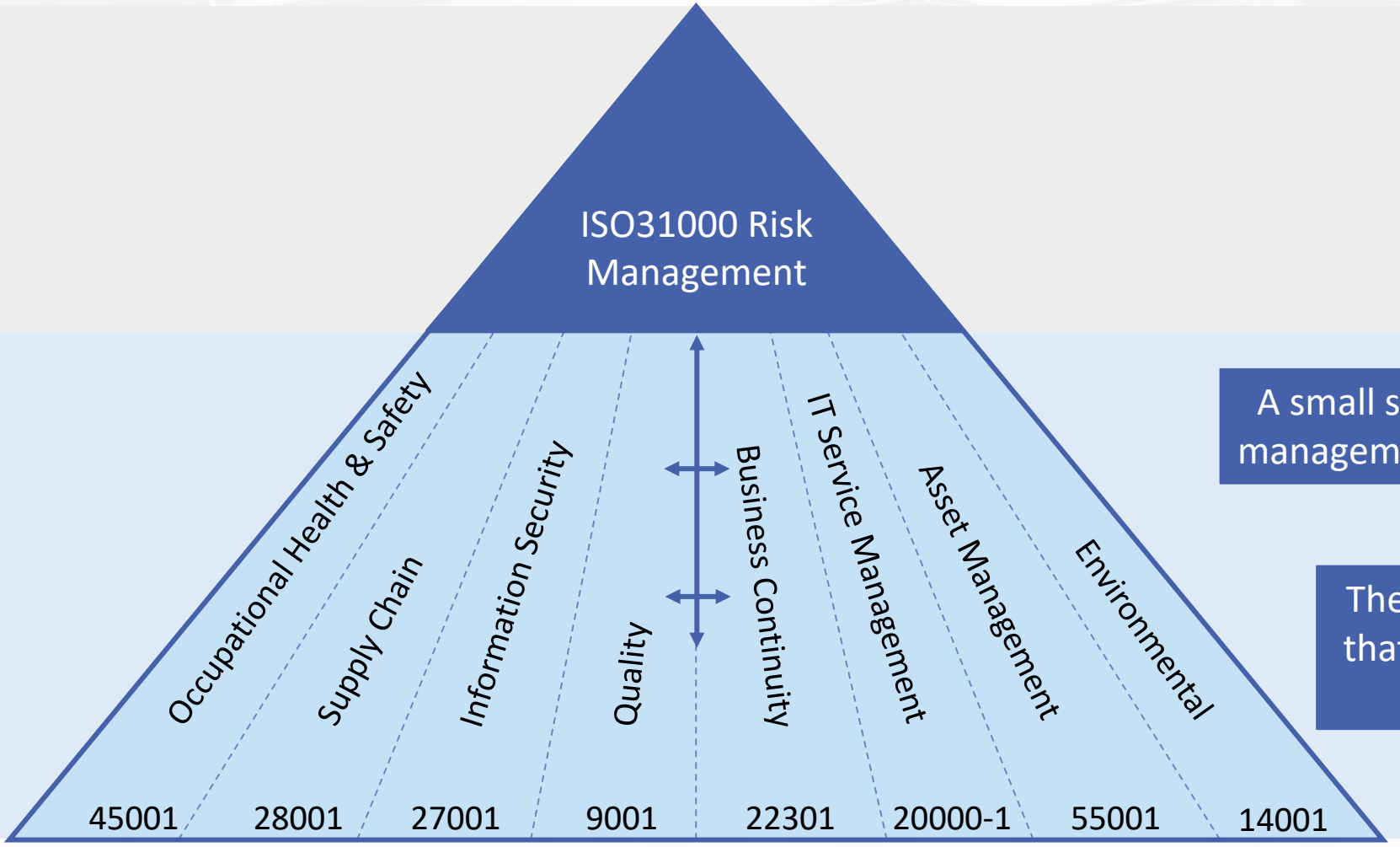
"The property of being accessible and usable upon demand by an authorised entity"

Source: ISO/IEC 27000:2014

WHAT IS A MANAGEMENT SYSTEM

- Set of interrelated or interacting elements of an organisation to establish policies and objectives, and processes to achieve those objectives.
- Systematically manages business risks.
  - Aligned with and in support of business objectives
  - A framework that enables the organisation to manage the achievement or control of those objectives
  - Designed to meet stakeholder needs, enhance reputation and image
  - Applicable to all teams and activities under the management system umbrella
  - A framework that can be used for business improvement and change
  - Built around the way the business works, not a standard

MANAGEMENT SYSTEMS



A small selection of management systems

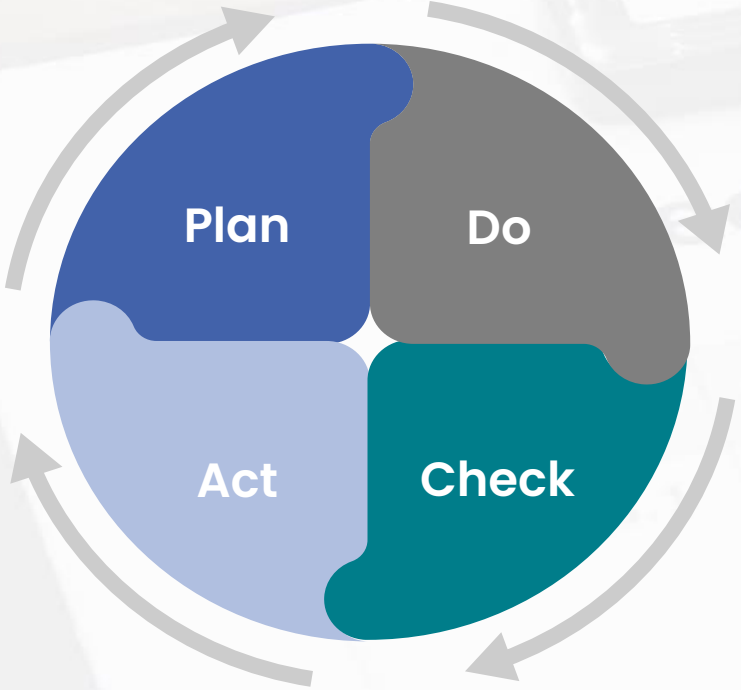
There are many others that may relate to your organisation

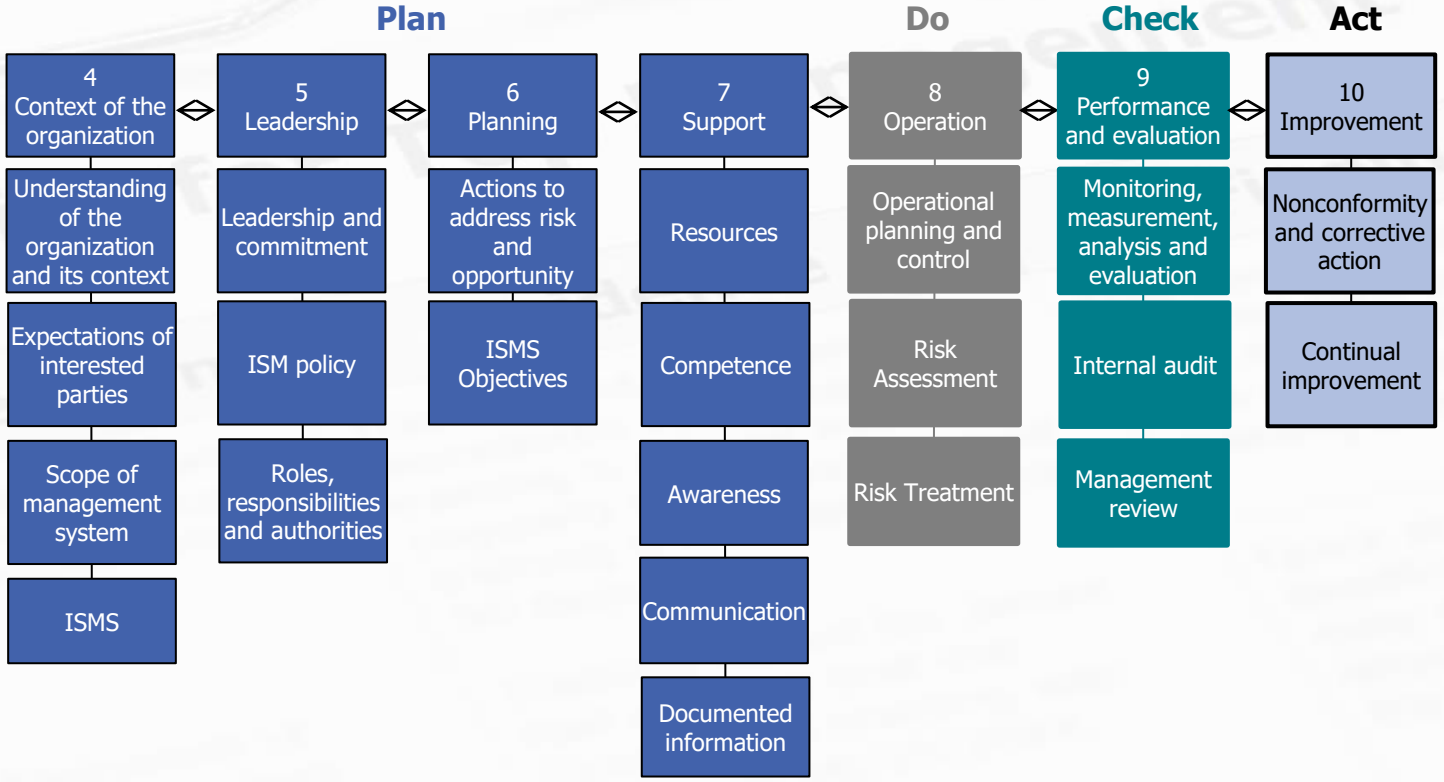
ISO27001 IS RISK BASED

- A key component of the standard is the risk assessment
- The risk assessment process aligns to ISO31000 so can be integrated into your organisational risk framework
- Context is key –need to understand the internal and external issues
- We only need to implement controls where we have risk (relates to rigor)
- This makes it very pragmatic and adaptable

- For example of the 93 controls in the new standard Resilient IT has implemented around 64 (removing a lot of the physical and secure development controls) – we are a virtual operation

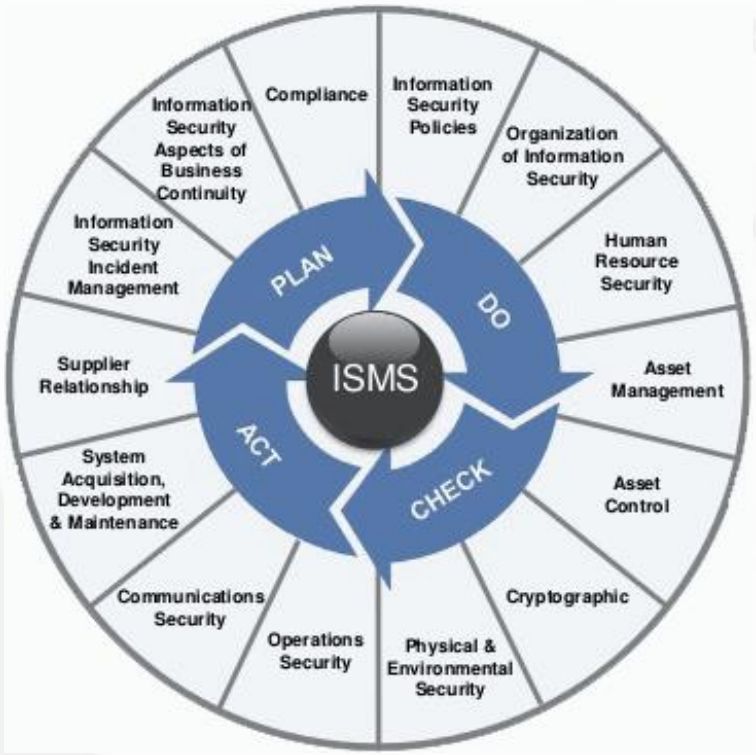
ISO27001: HIGH LEVEL STRUCTURE





ISO27001 CONTROL STRUCTURE

- ISO27001:2013 contains an Annex ‘A’ of controls that can be selected to mitigate risk
- This comes from ISO27002 which has been recently updated (simplified from 114 to 93 Controls)
- In ISo27002:2022 - 11 controls are new, 24 are merged, and 58 are updated



ISO27002:2013

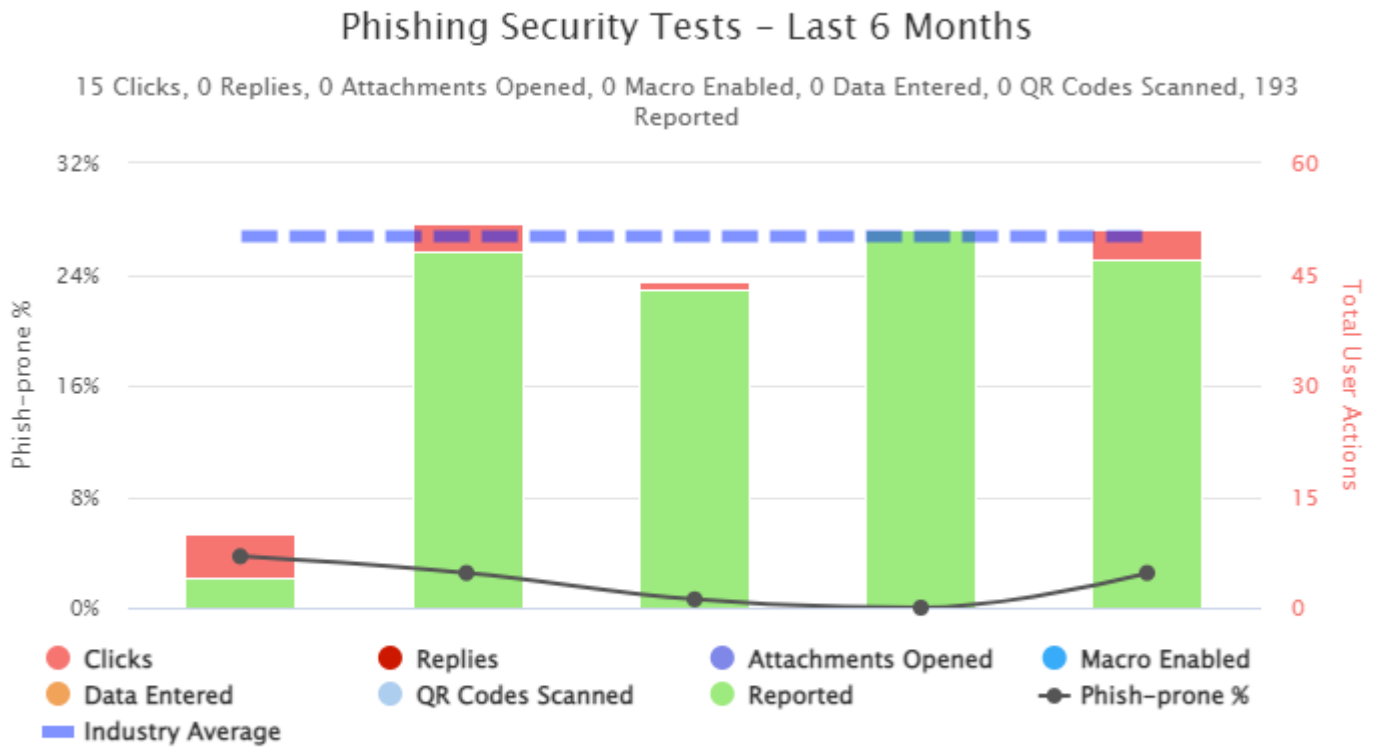
ISO27002:2022

INFORMATION SECURITY BASICS

1. **Control Applications:** Control which applications are allowed to run on systems to prevent any malicious activity.
2. **Patch applications and operating systems:** Keep applications up to date (makes them less vulnerable to attacks)
3. **Configure Microsoft Office macro settings correctly:** Sometimes malicious scripts are hidden in Microsoft files.
4. **User application hardening:** Ensure that web browsers block apps such as Flash and Java (a common exploit).
5. **Restrict administrative privileges:** Regularly evaluate who has administrator access to your systems
6. **Use Multi-factor Authentication:** Enabling MFA for all users significantly reduces risks of account compromise
7. **Daily backups:** Maintain regular offsite backups: 3:2:1 - 3 copies, 2 different mediums, 1 offsite.
8. **Use Disk Encryption:** Having Filevault or Bitlocker running significantly reduces the risk if a laptop is lost
9. **Password managers:** Use a Password Manager and generate unique complex passwords
10. **Training and Awareness:** Continually train staff they are your Human firewall –
11. **Don’t click dodgy stuff!!!**

PHISHING PROGRAMME

Phishing



Industry Benchmark Data

Account Average Phish-prone %	1.8%
Last Campaign Phish-prone %	2.5%
Industry Phish-prone %	26.7%

Industry Technology

Organization Size Small (<250 user

Program Maturity Baseline

Industry Benchmark Chart Data

TWILIO HACK

- August 8th
- Phishing

SECURITYWEEK
CYBERSECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe | 2022 CISO Forum | ICS Cyber Security Conference | Contact

Malware & Threats | Cybercrime | Mobile & Wireless | Risk & Compliance | Security Architecture | Security Strategy | ICS/OT | IoT Security

Home › Cyberwarfare

Twilio Hacked After Employees Tricked Into Giving Up Login Credentials

By Ryan Naraine on August 08, 2022

Tweet | Recommend 11 | RSS

Enterprise software vendor Twilio (NYSE: TWLO) has been hacked by a relentless threat actor who successfully tricked employees into giving up login credentials that were then used to steal third-party customer data.

The San Francisco company fessed up to the breach in an online notice that describes a sophisticated threat actor with clever social engineering skills and enough resources to switch carriers for ongoing text-based phishing attacks.

Twilio said the attack against its employee base succeeded in fooling some employees into providing their credentials. "The attackers then used the stolen credentials to gain access to some of our internal systems, where they were able to access certain customer data," Twilio added.

The company did not provide details on the extent of the breach, how many customers were affected, or whether the stolen data was encrypted and secured.

Twilio, a powerhouse in the enterprise communication API business with 26 offices in 17 countries, described the incident as ongoing and warns that the threat actor is sophisticated

Google™ Custom Search | Search

GET THE DAILY BRIEFING

BRIEFING

Business Email Address | SUBSCRIBE

Most Recent | Most Read

- SEC Charges 18 Over Scheme Involving Hacked Brokerage Accounts
- Iranian Group Targeting Israeli Shipping and Other Key Sectors
- Quarterly Security Patches Released for Splunk Enterprise
- The Future of Endpoint Management
- Security Analysis Leads to Discovery of Vulnerabilities in 18 Electron Applications
- Fugitive Arrested After 3 Years on Charges Related to BEC Scheme

QUESTIONS?

MORE INFORMATION

- www.thebci.org – Business Continuity Institute
- www.bsigroup.com – Certification, Audit and Training
- www.cert.govt.nz – Cyber Guidance
- www.resilientit.co.nz – That's Us ☺

ResilientIT

THANKS

Managing Risk – cyber insurance

Tanya Wood

18 August 2022

Risk

Current Trends
(from an insurance perspective)

- Significant increase in the number of notifications and claims that insurers are receiving for cyber attacks.
- More targeted and ambitious.
- Significant increase in frequency and severity of Ransomware attacks.
- Premiums and excesses will be increasing. Decrease in the cover available and lower limits.
- Cyber insurance still in its infancy.
- The mandatory reporting obligations which took effect from 2018 in Australia triggered the growth of the uptake of cyber insurance. We will likely follow the Australian trend.

Cyber insurance

What does cyber insurance normally cover?

- Cyber policies in NZ vary quite significantly.
- Is usual for the policies to cover:
  - Costs arising out of a:
    - **network security breach** (i.e. computer attack);
    - **privacy breach** and/or a;
    - **confidentiality breach**.

Coverage

Cyber insurance

What type of costs or losses are usually covered?

- The cost of the breach
- First party costs and PR costs incurred
- Loss of income
- Extortion or ransoms
- Loss caused by cyber crime (i.e. where there has been misuse of the businesses electronic identity):
  - cost of reimbursing customers for financial loss from fraudulent communications or websites designed to impersonate the insured / insured's products\;
  - loss of income caused by cyber crime
- Negligence – damages and defence costs raising from a claim alleging that the business failed to prevent a security breach or a privacy breach etc.
- Fines / penalties for a privacy breach (but not criminal penalties or fines).
- Usually a first response provider or first response network available.

Coverage

Cyber Insurance

What isn’t covered in cyber insurance?

- Claims made policies
- Loss or damage to physical property i.e. hardware
- Betterment:
  - only covers the cost to identify and fix software issues caused by the covered loss
  - will only restore systems to the same functionality as prior to the attack
- Loss caused by a failure in the design of any network or digital assets
- Loss caused by failure to maintain any computer, network or software
- Any amount which Insurers are prohibited from cover at law
- Any act of terrorism (look for cover for cyber terrorism or a definition of this)

Risk Management

Cyber incident management

National Cyber Security Centre (CERT) - Cyber incident management guide

- Ways organisations can protect their data, network and customer information.

*NCSC-Incident-Management-Be-Resilient-Be-Prepared.pdf

Risk Prevention

Key risk prevention recommendations

1. **Risk Assessment:**
   a. Services and assets
   b. Role of insurance

2. **Incident Response Plan:**
   a. How has your role as Privacy Officer been factored into your incident plan?
   b. Have you factored your insurance into your incident plan?
   c. When do you contact your insurer?
   d. What is the role of insurers in your incident plan?

Risk Mitigation

Risk Prevention

Practical steps to mitigate cyber risk – and why this is important for your cyber insurance

1. Incident response plan
2. Install software updates
3. Two factor authentication
4. Data backups
5. Set up logs
6. Update default credentials
7. Cloud service providers
8. Necessary Data only
9. Anti-malware software
10. Secure your network
11. Manual checks for financial details

Ransomware

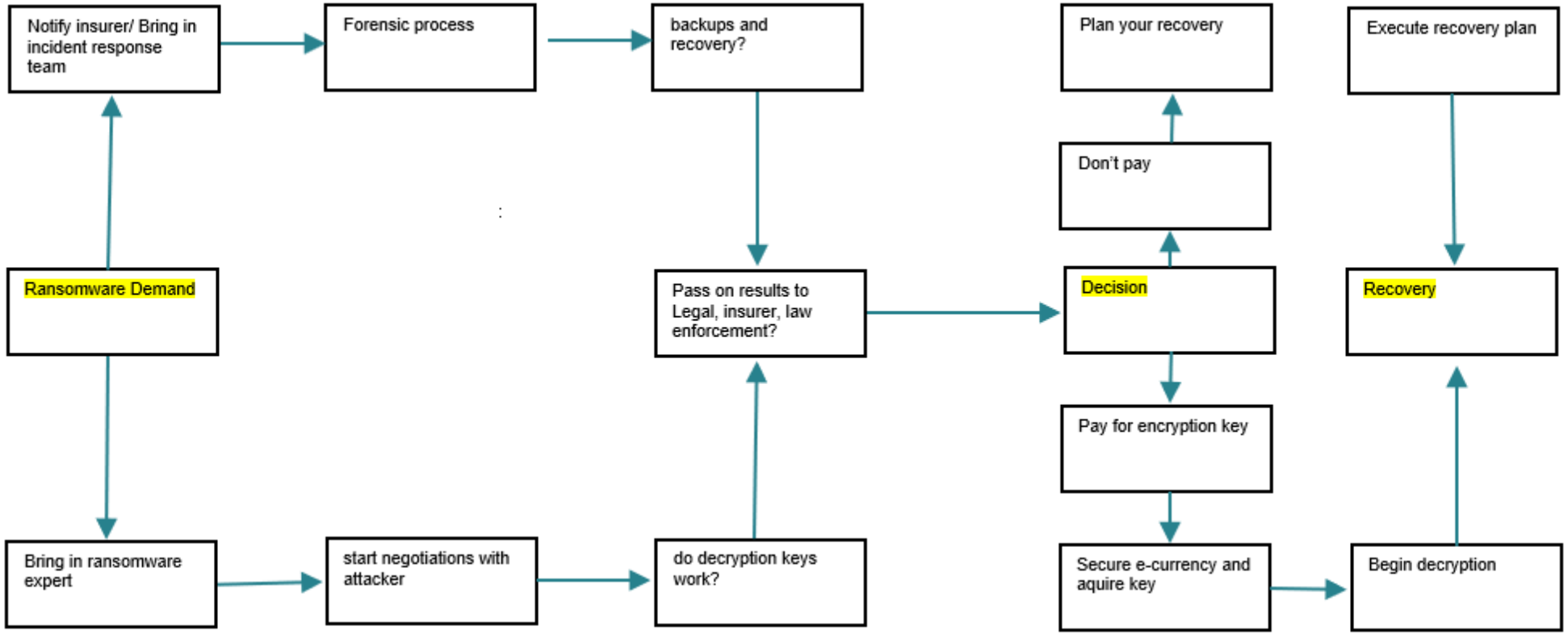
As part of your incident plan you should have a ransomware payment policy:

- You will need input from your legal counsel in particular how your insurance will respond (or not).
- Consider how you would pay a ransom – normally in bitcoin or e-currency
- If you pay you must comply with AML requirements

OFAC Sanctions

The role of your insurer

The first response process



Cyber insurance trends

Summary of trends in cyber insurance

1. Incident response plans:

- Growing importance for obtaining cover and cost of cover

2. Lawyers managing the first response:

- Cyber breaches / first response to be managed by external legal advisors
- Internal legal advisors (including Privacy Officers) to play key role in managing a breach

3. Cyber insurance:

- Less capacity
- More expensive / less cover
- More consistency between policies