

# How resilient are organisations to cyber incidents?

A survey on the current state of cyber resilience in organisations

Team Members

UQ: Elinor Tsen, Associate Professor Sergeja Slapničar, Professor Ryan Ko



#### **Research overview**

The World Economic Forum highlighted, in their recent *Global Cybersecurity Outlook 2022*, the importance of cyber resilience for all organisations.

Cyber resilience is especially important for critical industries.

However, there is some confusion around:

- (1) how cyber resilience differs from existing cyber security measures
- (2) what organisations are currently doing to develop cyber resilience

As part of a joint research project between the University of Queensland, Australia and Cloud Security Alliance Asia-Pacific, we conducted focus groups and a survey to understand the current state of cyber resilience in organisations. This e-brochure summarises the key findings from this survey.

In total, 108 individuals completed an online survey between October 2021 – February 2022. Respondents were involved in their organisation's cyber security or resilience management.

Research overview

Cyber resilience



#### **Research overview**

Based on the review of several prominent cyber resilience frameworks, this study is first to operationalise cyber resilience as a measurable research construct. We defined it with seven dimensions:

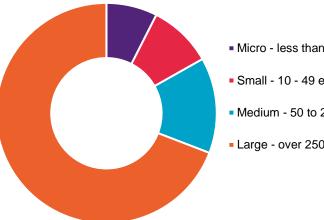
- 1) Prevention
- 2) Detection
- 3) Response
- 4) Recovery
- 5) Education
- 6) Leadership and accountability
- 7) Strategy and planning

We also investigated factors that affect the development of cyber resilience and cyber incidents that organisations experienced at a given level of cyber resilience.



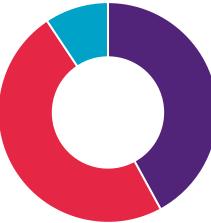
### Survey demographics

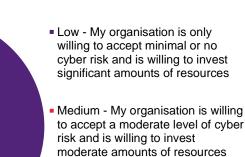
#### Organisation size



- Micro less than 10 employees
- Small 10 49 employees
- Medium 50 to 249 employees
- Large over 250 employees

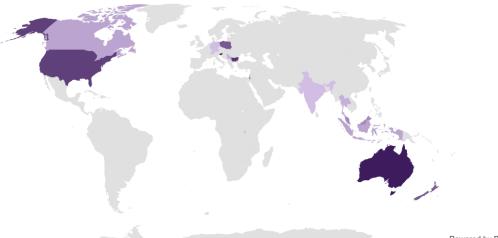
#### Cyber risk appetite





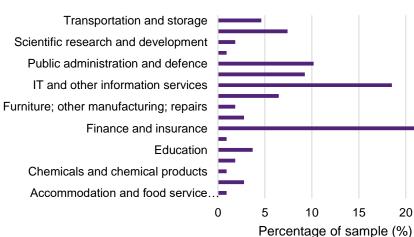
High - My organisation is willing to accept substantial cyber risk and is willing to invest relatively low amounts of resources

#### Geographic distribution of respondents



Powered by Bing © Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom, Wikipedia

#### Sector distribution of sample



#### Cyber resilience

#### Outcomes

20

25



## Survey results



### Cyber resilience score

As part of this study, we calculated an organisation's cyber resilience score.

Each question was assigned a score from 0 to 5 (5 representing Agree).

For each of the seven dimensions, the relevant questions were summated.

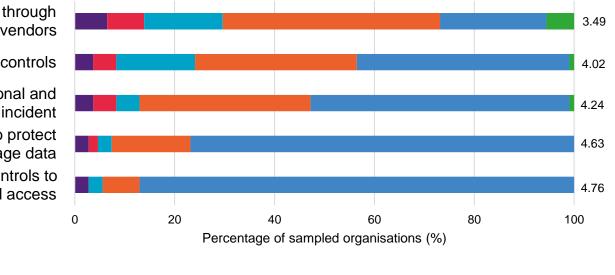
These summated scores were then standardised from 0 to 10 as each dimension was given equal weighting.

These scores were then presented to respondents as a percentage representing their score out of 70.

We have provided the average scores by sector for each dimension following the descriptive analysis.



### Prevention



My organisation develops controls across the supply chain through coordination with vendors

My organisation regularly reviews, tests and updates prevention controls

My organisation has developed and implemented organisational and technical redundancy to prepare for a cyber incident

My organisation implements technical and non-technical controls to protect and manage data

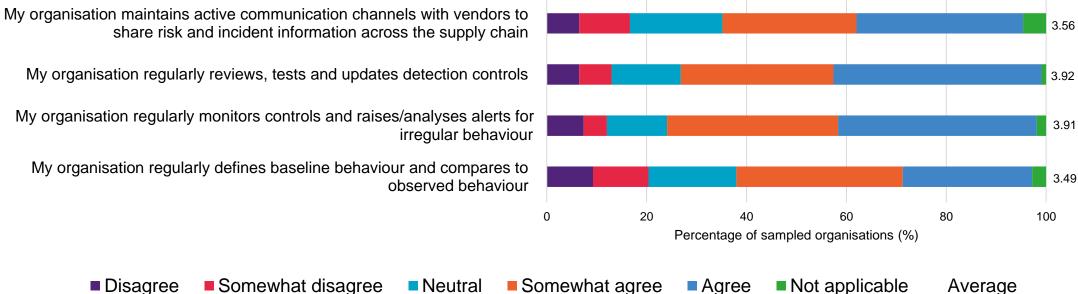
> My organisation implements technical and non-technical controls to prevent unauthorised access

Disagree Somewhat disagree Neutral Somewhat agree Agree Not applicable Average

- Prevention controls are the most frequently implemented controls.
- However, organisations appear to be implementing prevention controls in isolation ignoring the actions of other organisations.





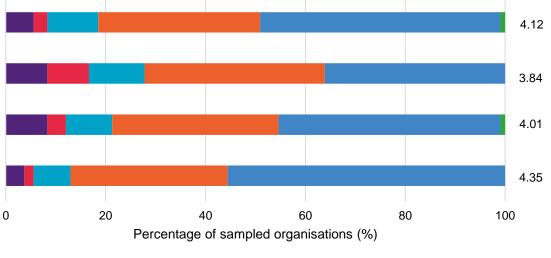


- The evaluation of detection controls appears to be more frequent than the defining of baseline behaviour.
- This either indicates expected behaviour may not change or organisations are behind when updating expected behaviour.
- This may have a run-on effect on what alerts are raised.

Research	overview
----------	----------







My organisation assigns responsibility to relevant individuals for steps within the response plans

My organisation develops and regularly tests technical and non-technical response plans

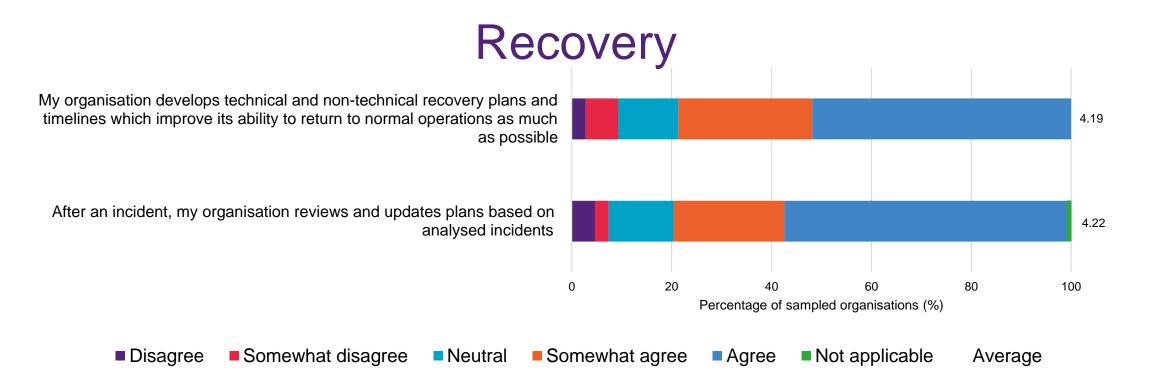
My organisation collects, assesses and shares cyber incident information with relevant internal and external stakeholders

My organisation responds to incidents in a timely and appropriate manner which is evaluated post-incident

Disagree Somewhat disagree Neutral Somewhat agree Agree Not applicable Average

- Most organisations are responding to cyber incidents.
- However, it appears to be similar to ad-hoc responses rather than planned responses.

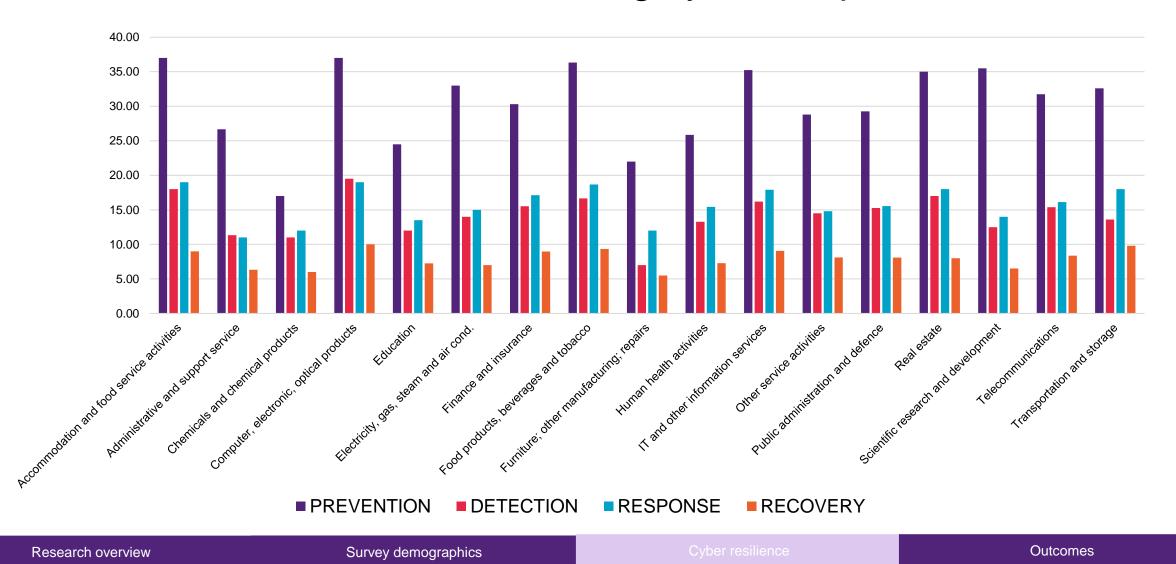




- The process of developing recovery plans is less frequent than expected.
- Organisations appear to be less focused on recovery than expected.
- This may indicate that the planning for cyber incidents stops at responding to the cyber incident.

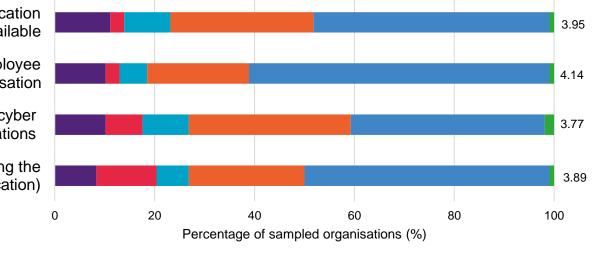


#### Prevention tends to be the most highly developed dimension









My organisation regularly reviews, evaluates and updates the education and training available

My organisation highlights, during training, that every employee contributes to a cyber secure organisation

My organisation ensures that training defines its approach to cyber security, procedures for failing to adhere to the training and expectations

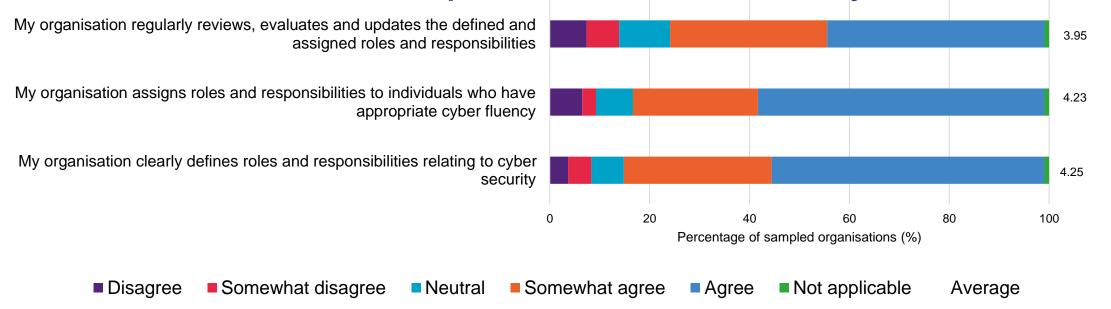
My organisation offers regular internal or external training (including the opportunity for cyber security certification)

Disagree Somewhat disagree Neutral Somewhat agree Agree Not applicable Average

- Education does not appear to be as much of a priority as expected; however employees are expected to
  contribute to the cyber security of the organization.
- This may indicate that the education program offered to employees may vary in detail but the expectations on employees do not change.

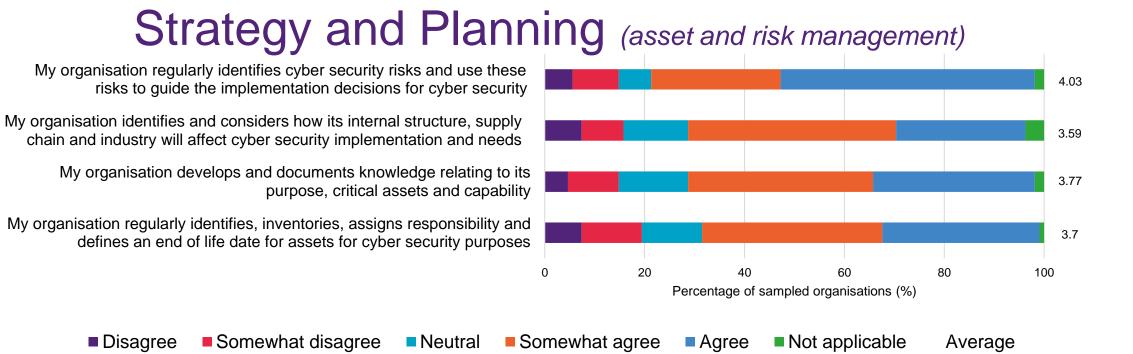


### Leadership and Accountability



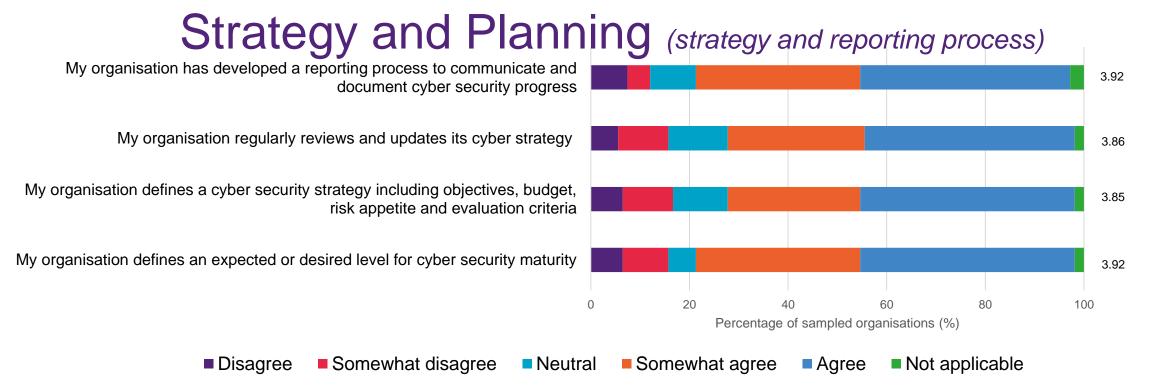
- The evaluation of cyber leadership roles is less frequent than expected.
- This may indicate that the accountability of cyber leadership may be lacking, which may not encourage optimal decision-making.





- Organisations do not appear to be frequently considering their internal structure and capabilities for cyber resilience.
- This reinforces the idea that cyber security, and cyber resilience, may be developed in organisations as onesize-fits-all.





- Most organisations are developing an appropriate strategy and reporting process.
- This indicates that this area of cyber resilience may be becoming a focus for cyber leadership.



#### Average education, leadership and accountability, strategy and planning score by sector

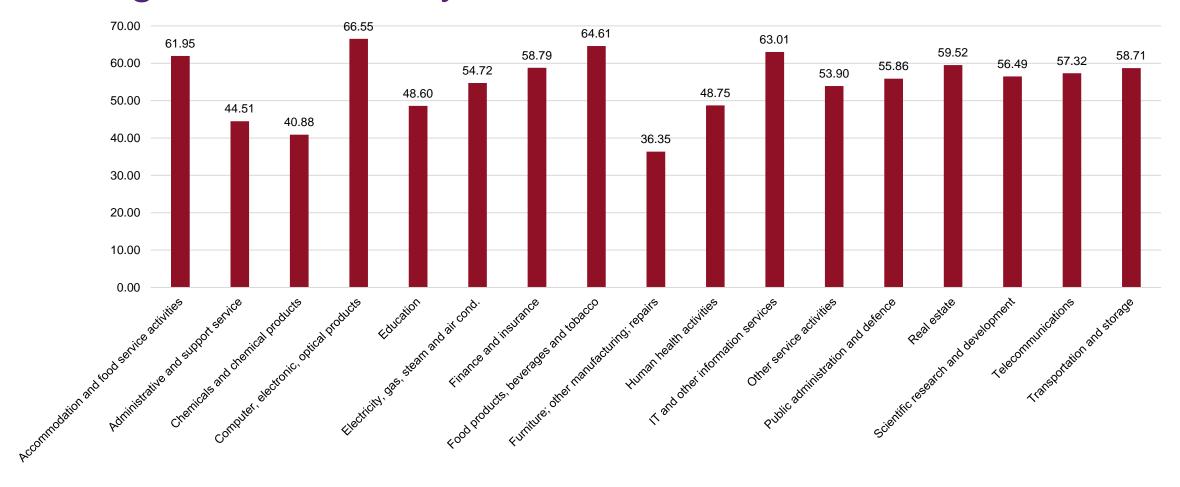


STRATEGY & PLANNING LEADERSHIP & ACCOUNTABILITY

Survey demographics



#### Average total score by sector





### Scores by sector summary

Highest average scores for prevention and strategy and planning This may indicate that organisations perceive these two dimensions as the most important

Recovery has the smallest average score across sectors

This dimension is still lacking across organisations indicating that the focus is not on recovering post-incident but on preventing cyber incidents

Education and leadership and accountability are also smaller than the other dimensions

Unexpectedly, the human factor for cyber resilience is still an issue despite the historical focus of cyber security and resilience

Detection and response appear to have similar average scores across sectors

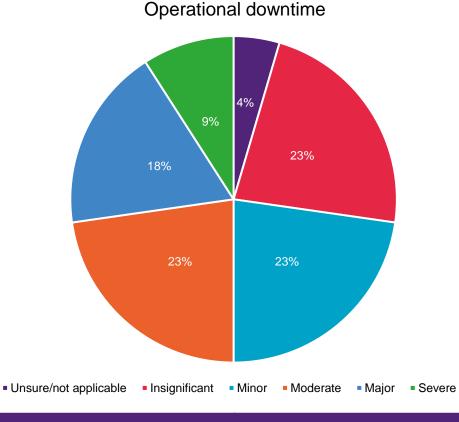
The best performing sectors overall are

- Computer, electronic and optical products
- Food products, beverages and tobacco
- IT and other information services
- Accommodation and food services
- Real estate

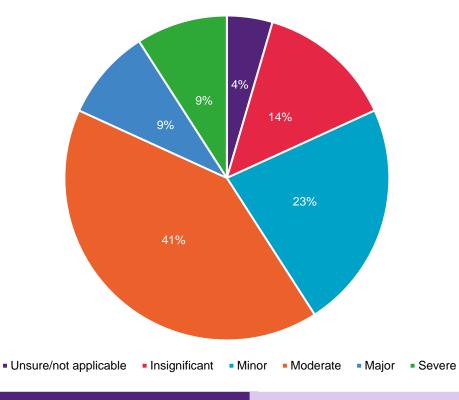


### **Outcomes - Organisation**

- Only 20% of organisations suffered a cyber incident they were willing to disclose
- Most cyber incidents were categorised as DDOS, phishing and ransomware
- Major negative outcomes were uncommon (less than 25%)



Inability to deliver value proposition (protecting human life, achieving organisational goals, etc.)



Survey demographics

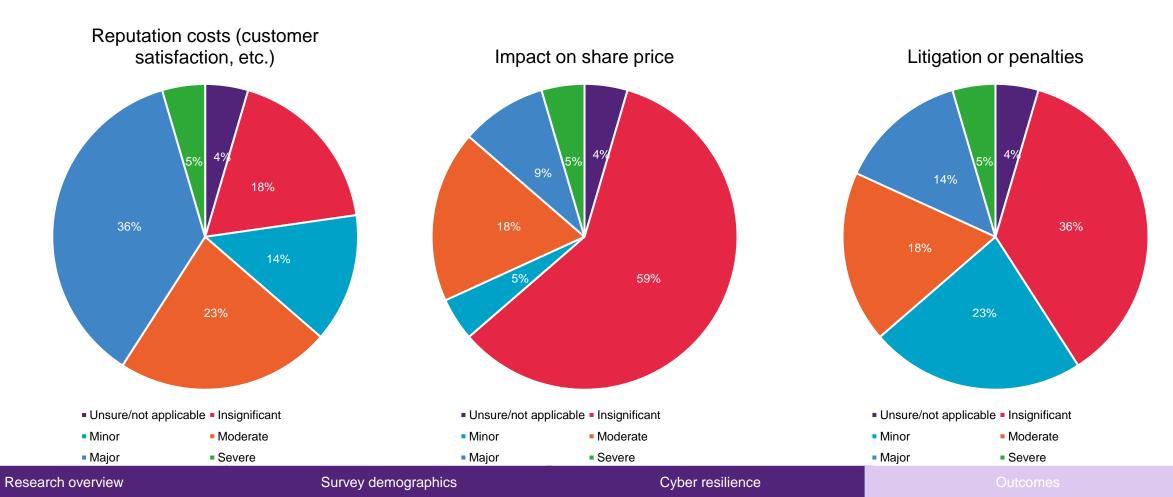
Cyber resilience

Outcomes



### **Outcomes - Reputation**

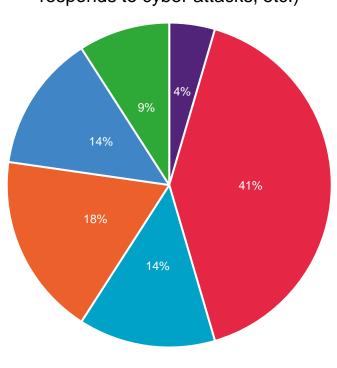
- Most organisations experienced an insignificant impact on share price post-incident
- Major negative customer costs were relatively common





### **Outcomes - Financial**

• Most organisations had significant financial costs (55%)



Financial costs (including insurance premiums and costs to responds to cyber attacks, etc.)

Unsure/not applicable
 Insignificant
 Minor
 Moderate
 Major
 Severe

lesea	rob /	DV/ORV	
			1011

Survey demographics

Cyber resilience



### Cyber resilience and outcomes

We analysed the results using a statistical method called MANOVA (*multivariate analysis of variance*) and found the following:

- Prevention affects operational downtime and ability to deliver value proposition.
- Prevention affects reputation costs, impact on share price and occurrence of litigation or penalties.
- Overall, strategy and planning appears to be important for organisations after a cyber incident.

#### Implications

- Our research shows that prevention and strategy and planning are two most highly developed dimensions. Having good prevention controls, particularly redundancy, is important in allowing the organisation to continue operating post-incident. In addition, organisations with good prevention controls are perceived more favourably as it is then apparent that the organisation is attempting to be cyber resilient.
- However, strategy and planning controls are also relevant. Generally, strategy and planning are important in providing evidence to stakeholders in showing that an organisation is attempting to be cyber resilient
- This does not mean that other dimensions are not as important for cyber resilience. Our findings may indicate that some dimensions are valued more by stakeholders than others.