Australian Government
Department of Home Affairs

CYBER AND INFRASTRUCTURE SECURITY CENTRE

Cyber and Infrastructure Security Conference March 2023

Exercise Insights

Summary

On 24 March 2023, the Cyber and Infrastructure Security Centre hosted a cyber security exercise (the exercise) as part of the inaugural Cyber and Infrastructure Security Conference (CIS conference). The conference was attended by approximately 1500 participants (500 in-person and 1000 online).

The exercise was co-facilitated by Joe Smith, A/g Assistant Secretary, Cyber Security Response Coordination Unit and Seth Enoka, Principal Incident Responder from Dragos. The exercise was developed by the CISC with support from Dragos and advice from a range of government and industry stakeholders.

The exercise was a discussion exercise and included in-person participation for those attending the conference and a facilitated online discussion for those attending remotely.

The objectives of the exercise were to provide participants with:

- an introduction to the discussion exercise format,
- insights into the different considerations faced by an entity responding to a cyber incident,
- an opportunity to network with colleagues across industry and government,
- considerations for their own organisation's incident response plans, and
- enable participants to identify commonalities to incident response between similar organisations.

The exercise focused on the non-technical response to cyber incidents. It included prioritisation for the different elements of response and the interactions between industry and government agencies.

The exercise provided key insights into how participants expected three following primary groups of stakeholders to respond to a cyber security incident.

- **The impacted entity** must respond to the cyber security incident, support impacted clients and customers, and engage with Australian Government stakeholders, the public, and other industry participants.
- **Impacted clients** are affected by disruptions to their services that significantly impact operations. They are concerned with managing the impact and engaging with clients and stakeholders, including the impacted entity, and Government.
- **Government** is concerned with the national response to the incident including public messaging, and any regulatory obligations relevant to the incident and entity.

Key Insights

The exercise provided some key insights into how participants expected relevant stakeholders to operate in response to the cyber security incident.

Key insights relating to the **impacted entity** included:

- impacted entities should establish multi-disciplinary teams – including representatives from third party service providers – to respond to the various aspects of a cyber security incident;
- boards and CEOs (both 34 per cent) and senior leadership teams (25 per cent) would be the key decision-makers;
- clients and customers should be the key focus:
    - impacts on them were the highest concern (4.4 out of 5),
    - communicating with them was the top priority (91 per cent),
    - customer relations teams should be involved in incident response (75 per cent), and
    - financial implications (2.09 out of 5) and reputational harm (2.22 out of 5) were the lowest concerns;
- cross-industry information sharing (52 per cent) was lower than expected; and
- the impact of incident response activities on staff are a concern.

Key insights relating to **government** included:

- the importance of impacted entities notifying the Australian Cyber Security Centre (99 per cent), reporting to regulators (83 per cent), and engaging with the Australian Federal Police (72 per cent).
- a coordinated response should include the impacted entity (99 per cent), operational agencies such as the Australian Cyber Security Centre and the Australian Federal Police (99 per cent), regulators (89 per cent),and emergency management agencies (54 per cent), among others.
- government needs to know about the actions the impacted entity has taken to respond to the incident (94 per cent), the interdependencies between impacted assets (84 per cent), and the impacted entity's public communications (75 per cent).

Key insights from the **context** of the exercise (i.e. that it was soon held after the Optus and Medibank data breaches) included:

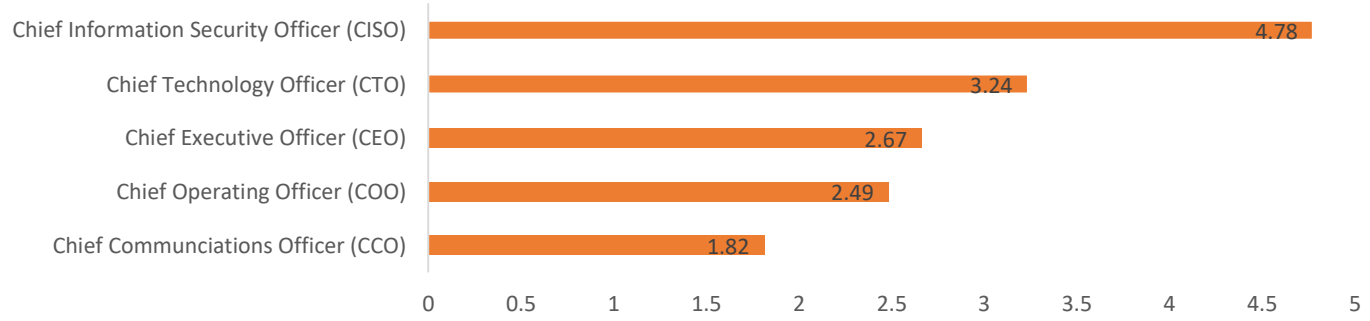
- a major focus on data issues following recent high profile data breaches:
    - government needs to know about exfiltrated data (95 per cent); and
    - exfiltration of sensitive data was the third highest concern (4.02 out of 5); and
- nearly all participants were unwilling to pay a ransom in response to an incident (95 per cent).

Exercise responses

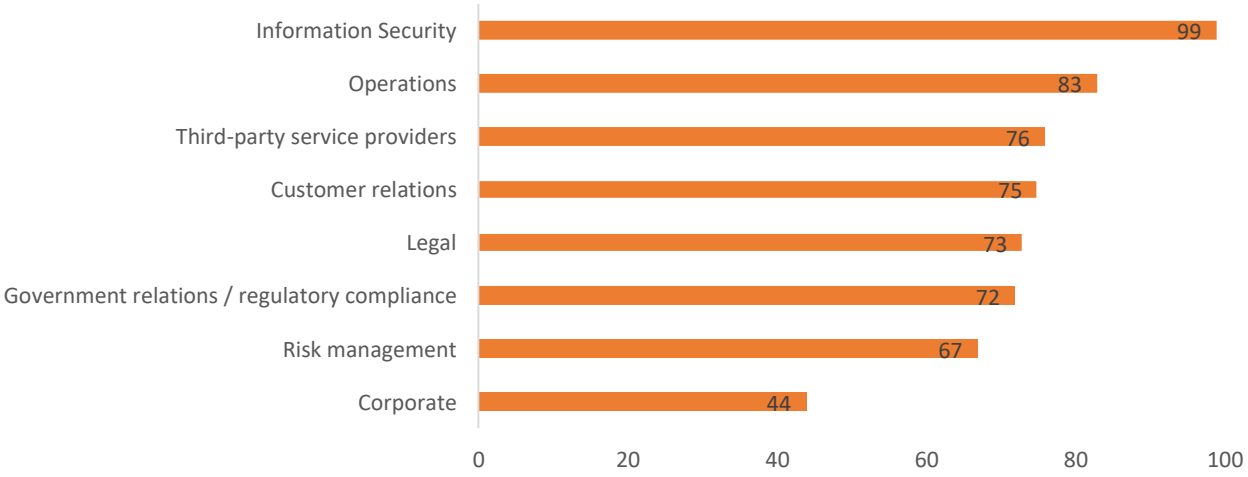
Inject 1: Initial response

A major Australian bank identifies that its Information Technology (IT) networks have been encrypted by a malicious cyber actor in a ransomware attack and is rendered unusable. Client data has been accessed. The bank's IT team is investigating the breach and analysing the data. The bank commences containment activities to secure adjacent networks.

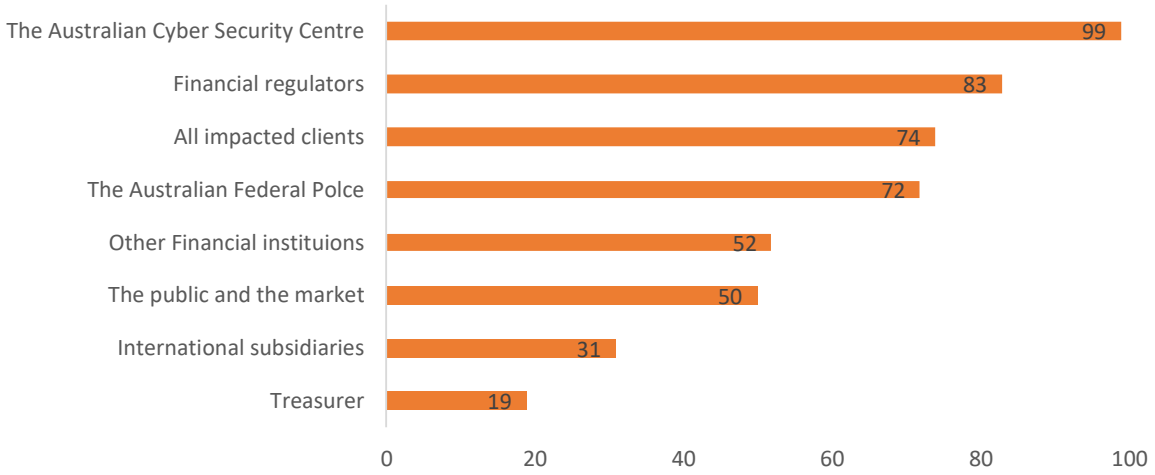
Question 1: Which of the bank's senior executives should be informed of incident when it is initially detected?



Question 2: Which organisational areas of the bank need to collaborate on the initial response to the incident?



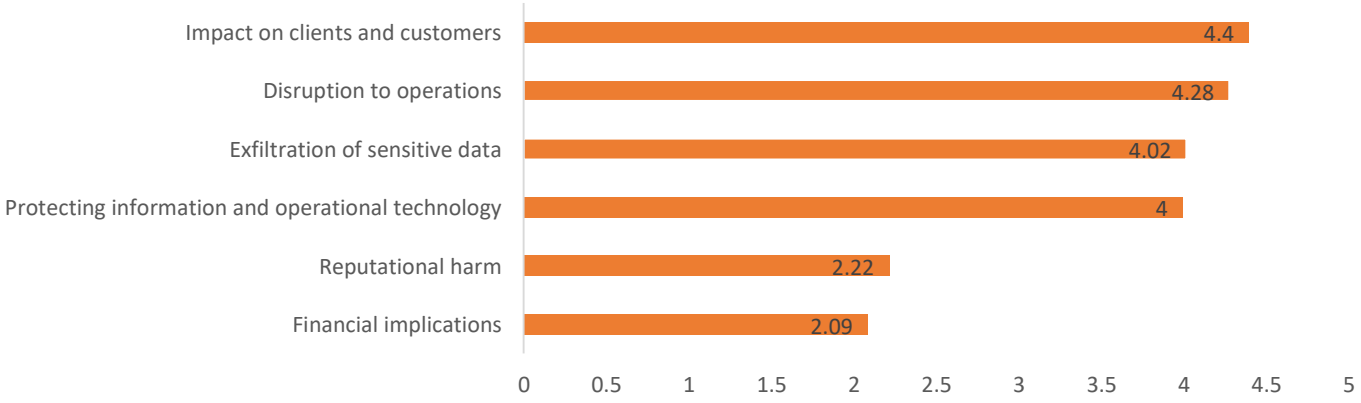
Question 3: Which stakeholders should the bank inform about the nature of the cyber security incident?



Inject 2: Escalation

The bank finds a ransom note. The actor is demanding a payment to decrypt the bank's network and delete copies of the data within 48 hours. Without payment, the actor claims they will release data including addresses, phone numbers and account details on the dark web. The bank begins to experience some critical outages in their Operational Technology (OT) across Australia. These outages are creating some unease across major cities as payment processing becomes intermittent and unreliable, and ATM's across the country are no longer operational, preventing access to funds for millions of customers. The disruption is also impacting a range of secondary critical infrastructure including: grocery services, transportation, telecommunications, and other financial sector services and data storage.

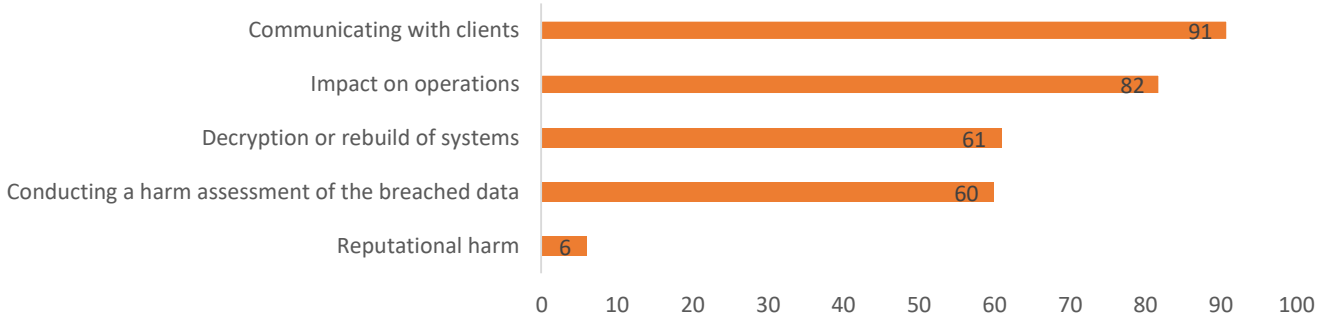
Question 1: Which of the below is the most concerning for the affected bank?



Question 2: Are there any other concerning factors for the affected bank that were not mentioned in the previous question? (Answers provided in open text form – *key themes reflected below*)

- Impact upon connected business and stakeholders
- Skills and capabilities to respond to the incident (immediate, medium and long-term)
- Internal and external communications
- Share price, reputational and legal risks
- Physical security (for staff) and reassurance of system security following remediation

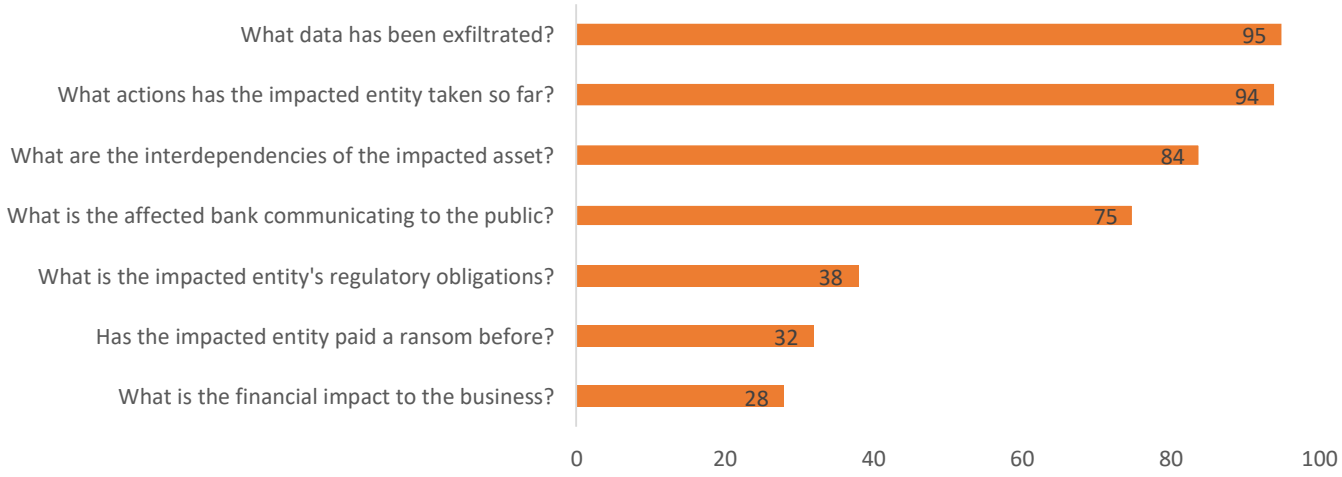
Question 2: Which aspects of the incident should the bank prioritise?



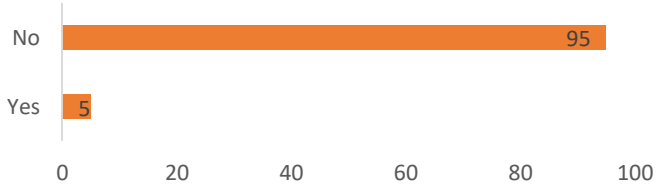
Are there any other aspects of the incident that the bank should prioritise that were not mentioned in the previous question? (Answer in open text form - *key themes reflected below*)

- Impact upon staff
- Ensuring containment, remediation, and business continuity
- Preservation of forensics/investigation
- Reporting to government and regulators
- Legal and community issues

Question 3: What information does Government NEED to know about the incident?



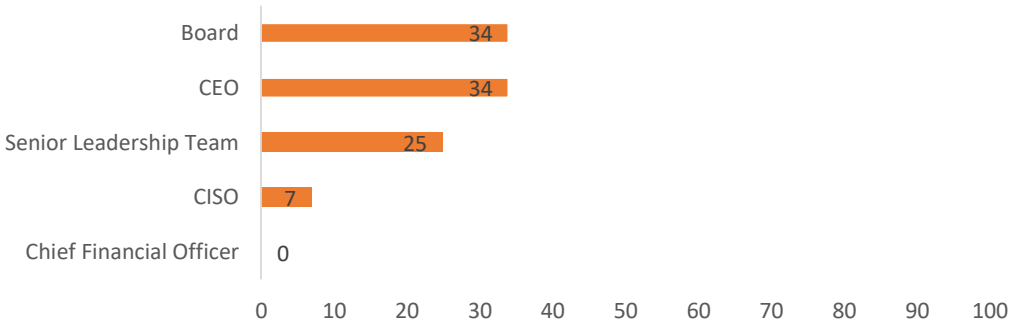
Question 4: At this stage of the incident, as the affected bank, would you pay the ransom?



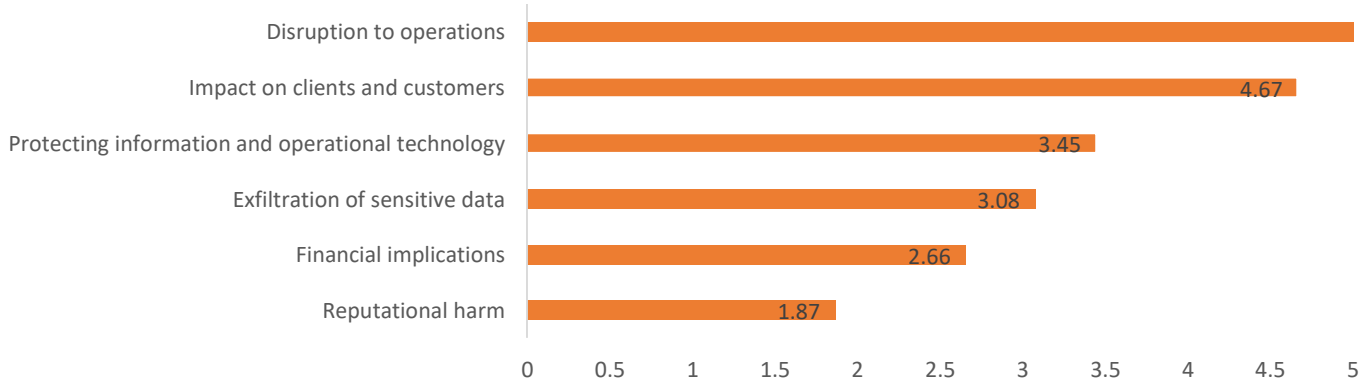
Inject 3: Response

The bank's service provider notifies the bank that a security researcher has developed a decrypter for this ransomware variant. However, decrypting systems will take several days, during which time the bank's services will be unable to operate across the country. If the bank does not use the decrypter, it will need to manually rebuild some key systems, which could lead to some systems being brought online earlier than the use of the decrypter. The actor has also published a sample of the client data on the dark web to confirm the exfiltration.

Question 1: Who should make the decision on whether the bank uses the decrypter or rebuilds its network?



Question 2: Which of the below is most concerning for impacted critical infrastructure clients? (e.g. a major supermarket)



Question 3: Who should be involved in the coordinated response?