Government of **Western Australia**
Department of **Finance**

# Welcome to the

# Strategic Procurement Community of Practice

Government of **Western Australia**
Department of **Finance**

The Department of Finance acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community.

We pay our respects to all members of the Aboriginal communities and their cultures; and to Elders both past and present.

Government of **Western Australia**
Department of **Finance**

# Today's program

**Big Game Hunting and the Evolution of Ransomware**

Dr Mohiuddin Ahmed – Edith Cowan University

**Cyber Risk Considerations in Procurement**

John Edwards– Office of Digital Government

Q&A

Networking

# Please welcome

**Dr Mohiuddin Ahmed**

**Senior Lecturer of Computing and Security**

Edith Cowan University

AUSTRALIA
ECU
EDITH COWAN UNIVERSITY

Creative
thinkers
made here.

# Big Game Hunting and Evolution of Ransomware!


## Dr Mohi Ahmed JP
## Senior Lecturer of Computing & Security

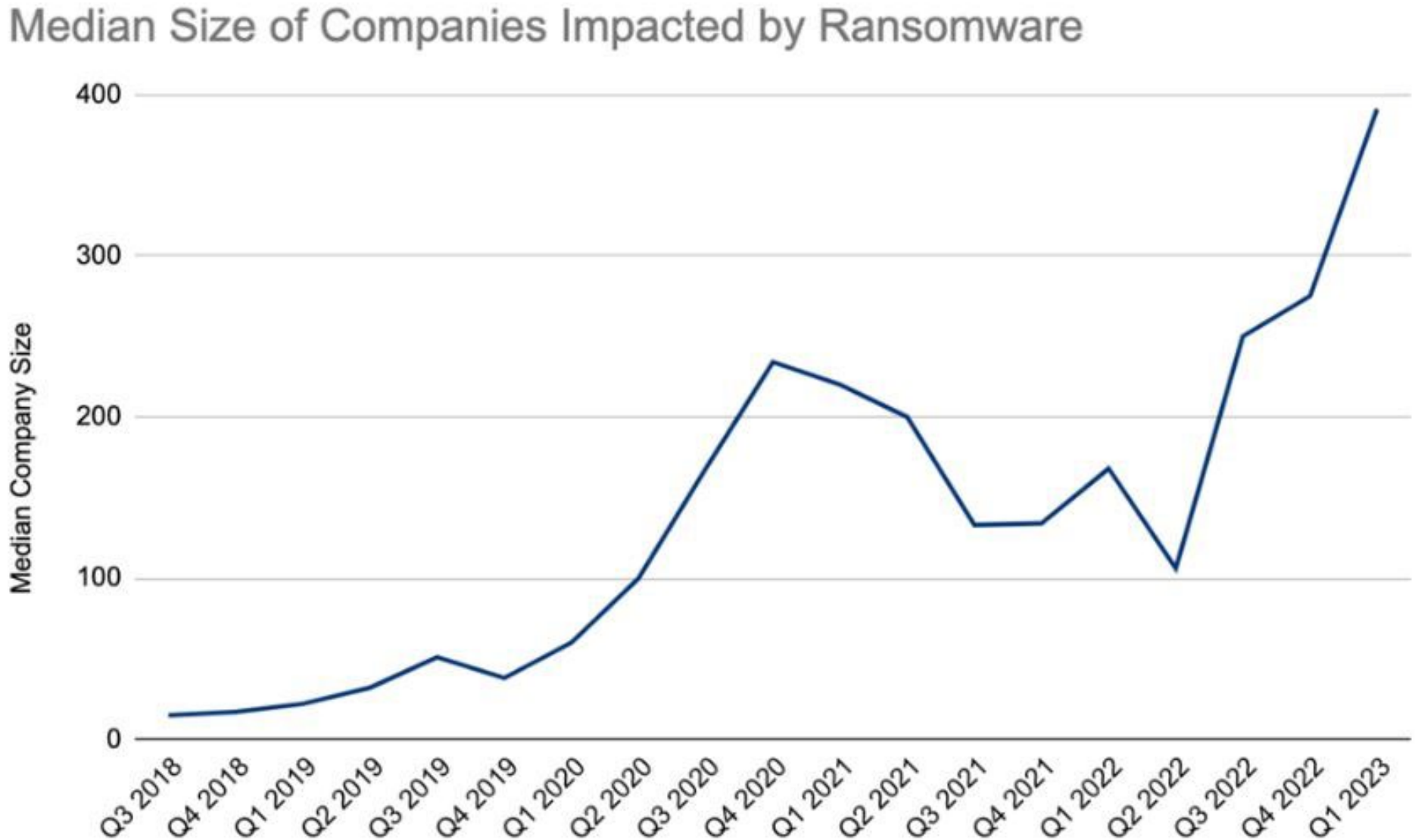
# Disclaimer

- The presentation is prepared in my personal capacity.
- The opinions in this presentation are my own based on years of research and teaching experience.
- Information shared during this presentation are from conventional and unconventional media sources.
- Like any human, I can be wrong sometime.

# Big Game Hunting

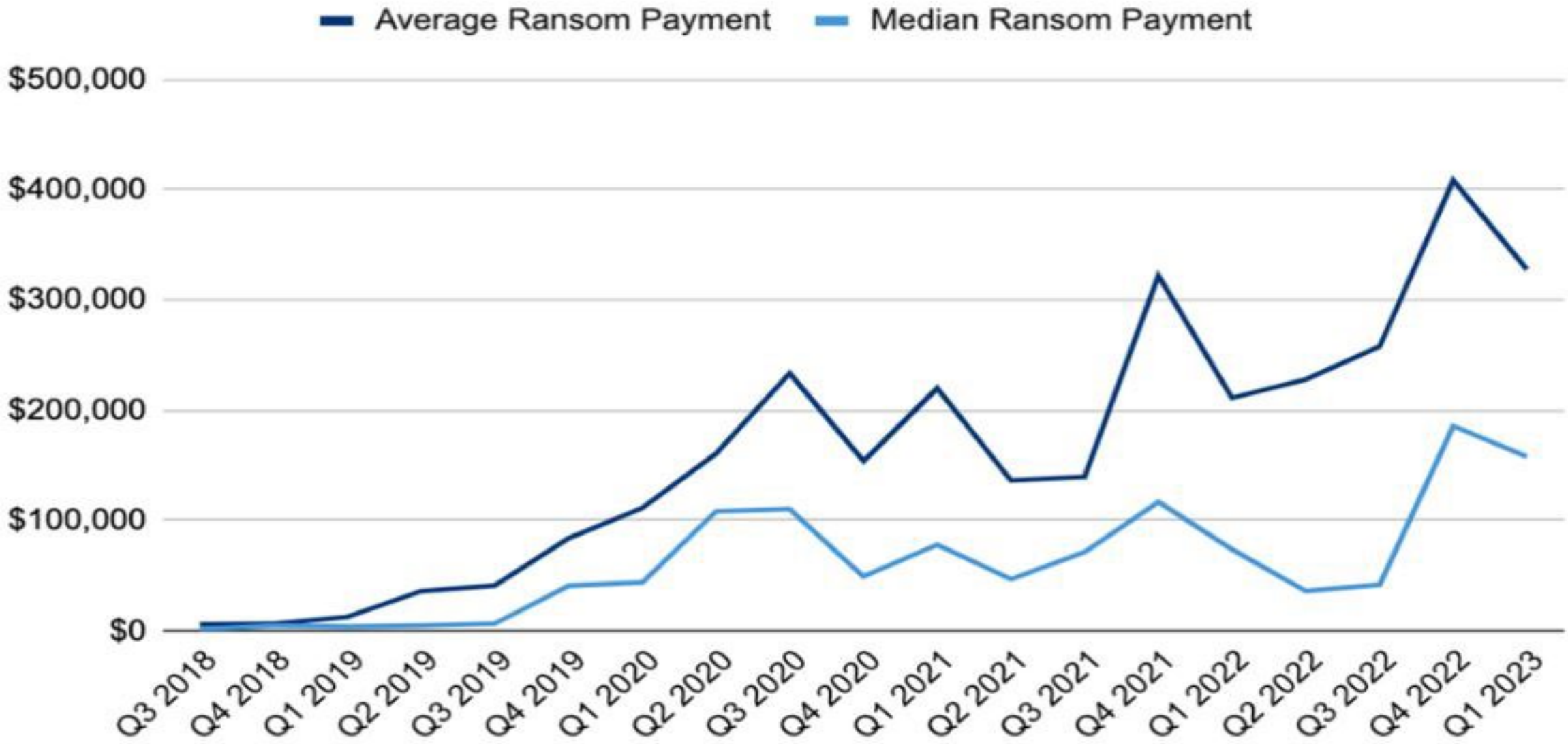
Hackers target large firms instead of smaller organizations and individuals.

Hackers are aware that larger enterprises with critical infrastructures can afford to pay higher ransoms.




Source: coveware.com

# Ransom Payments By Quarter

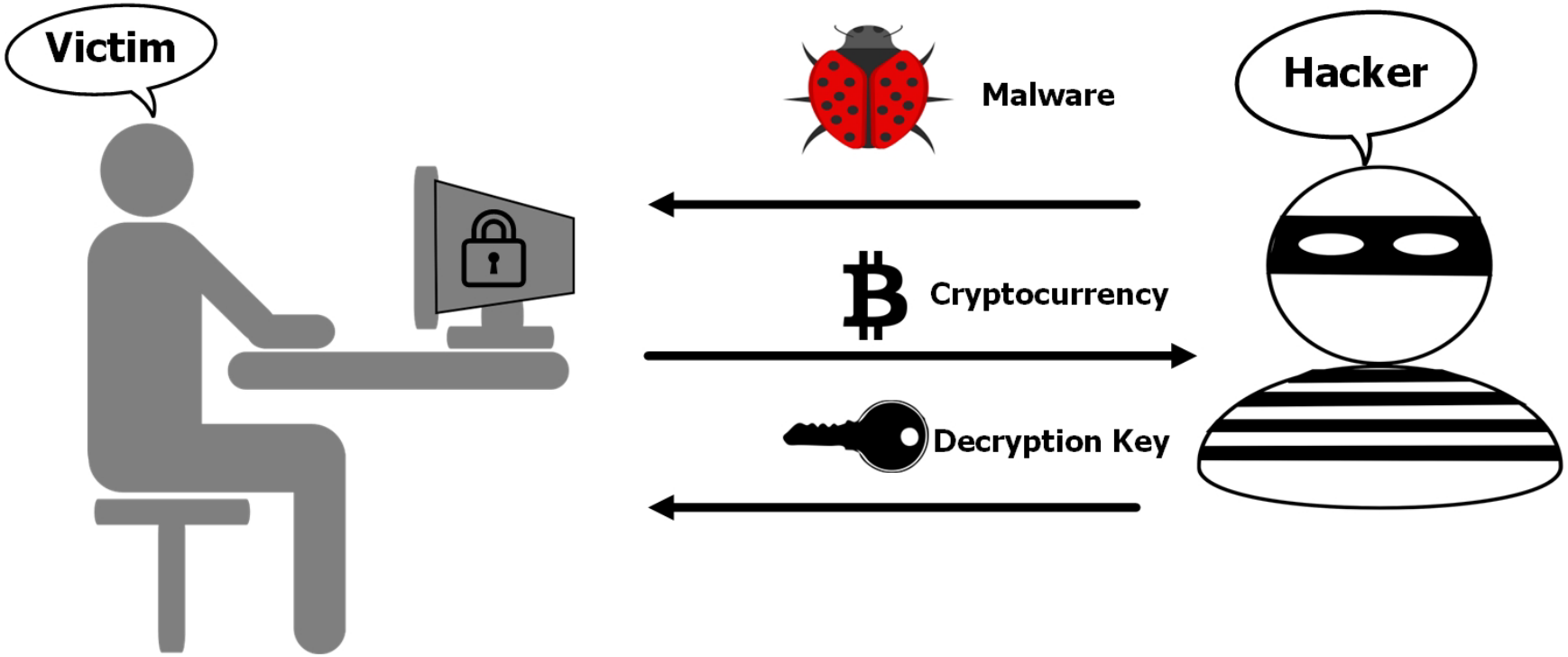



COVEWARE

# Evolution of Ransomware

AUSTRALIA ECU EDITH COWAN UNIVERSITY

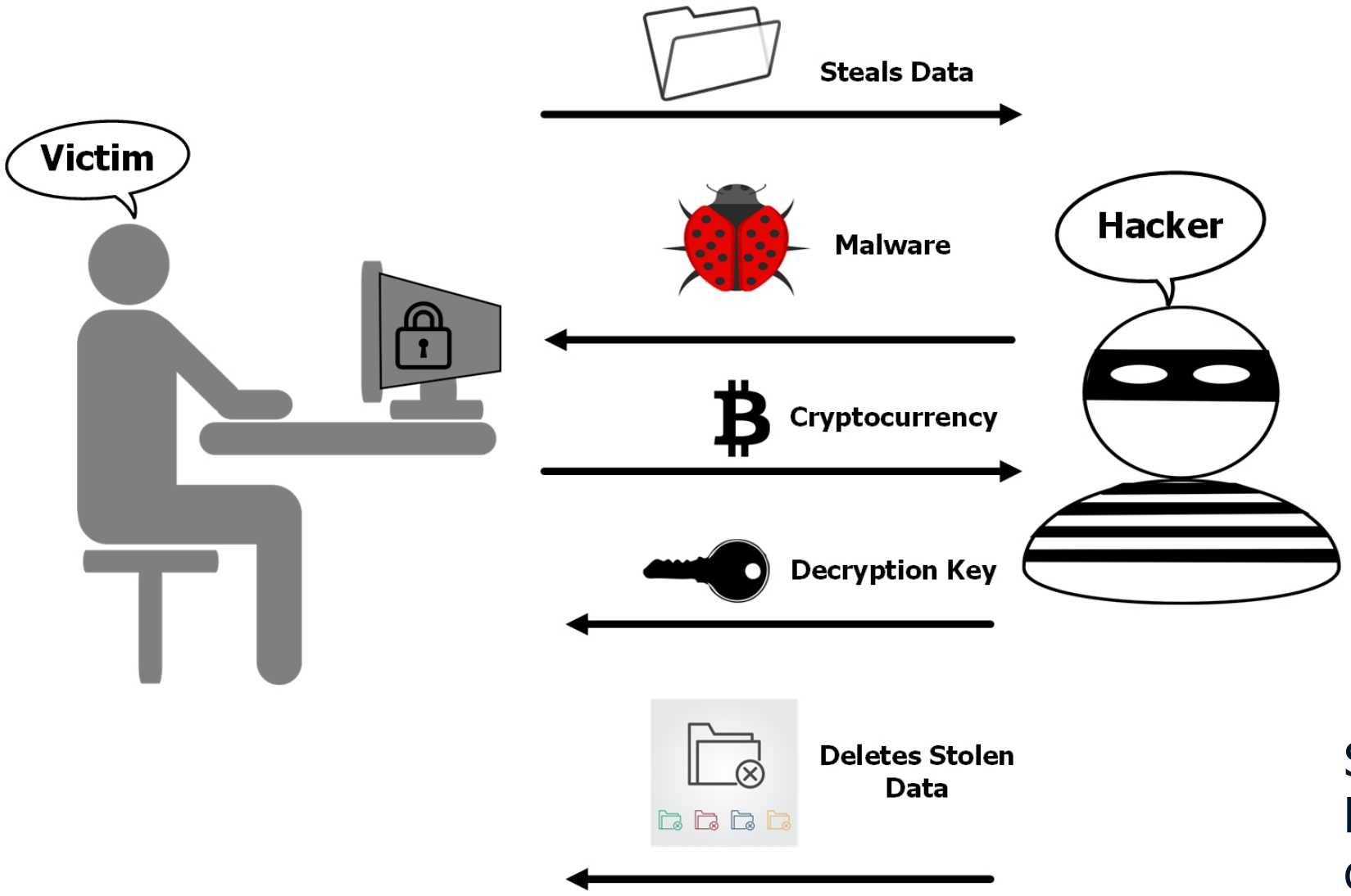
# Ransomware




Locks and ask ransom for the decryption key.

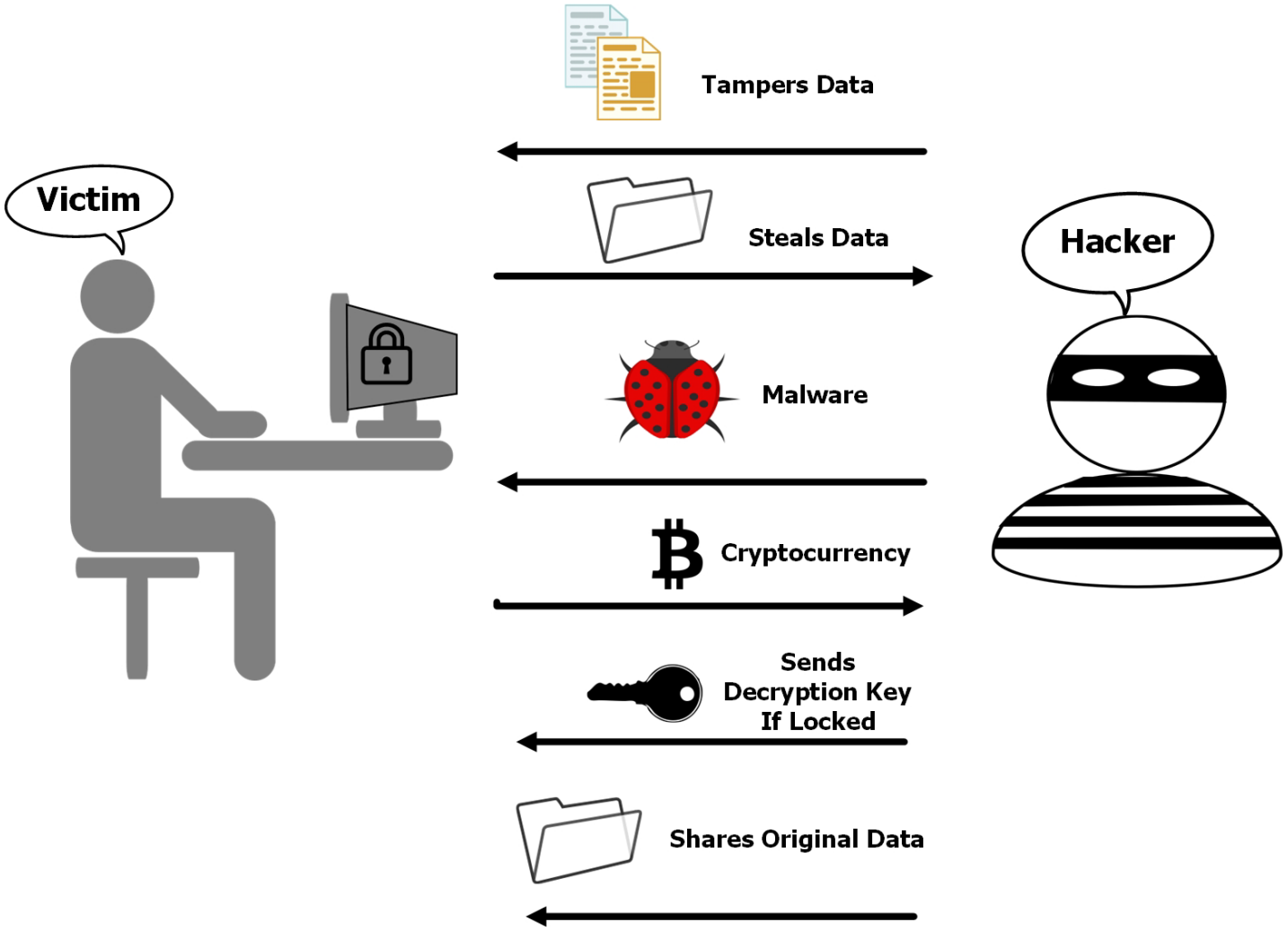
# Ransomware 2.0






Steals the data, ask ransom for both the decryption key and data.

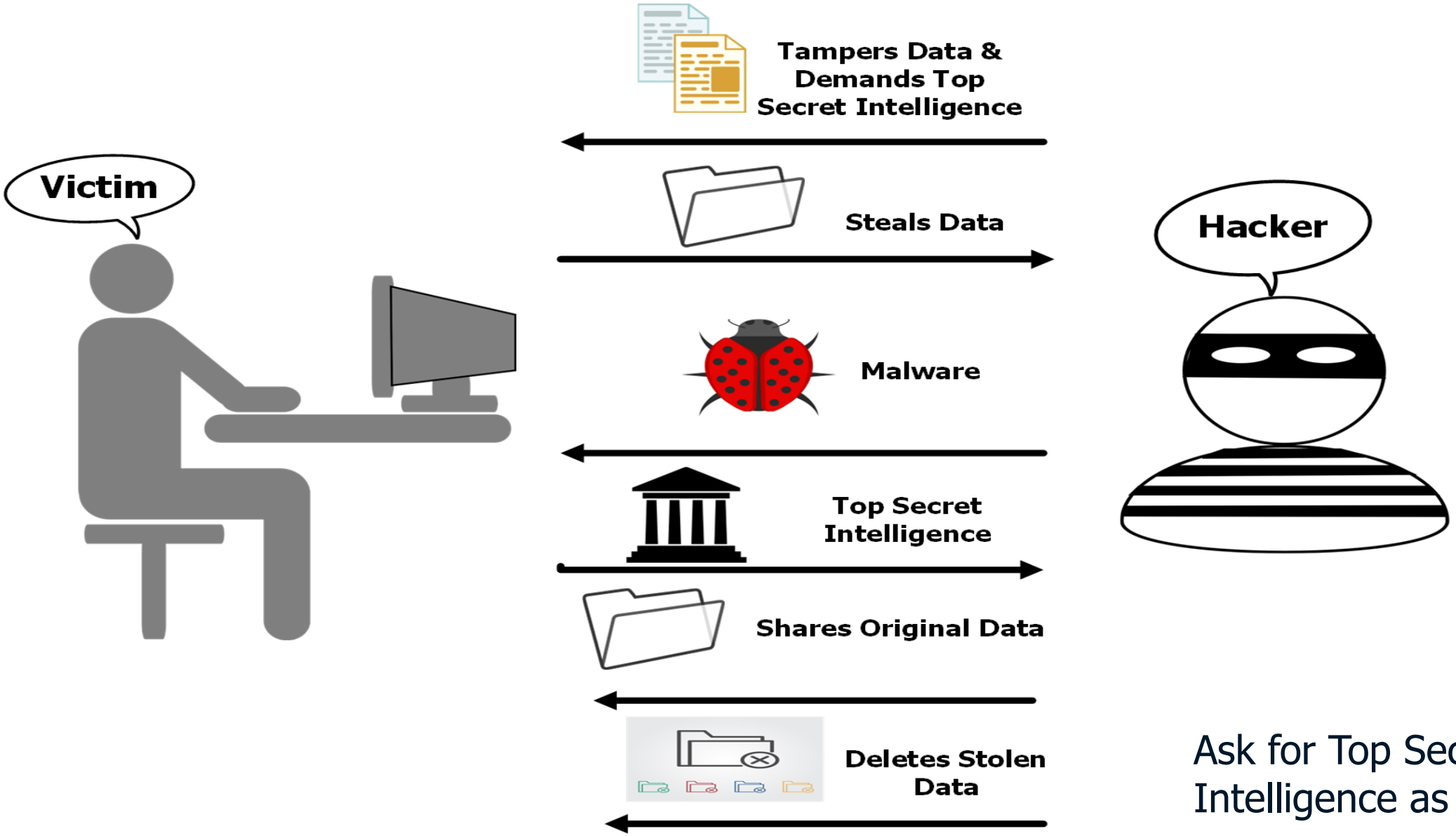
# Ransomware 3.0




Steals the data and keep a copy of the original, then tampers the data on victims' devices and ask for higher ransom!

# Ransomware 4.0






Ask for Top Secret Intelligence as Ransom!


OH SNAP!


It’s being called Russia’s most sophisticated cyber espionage tool. What is Snake, and why is it so dangerous?

# Cyber Espionage Tool developed by Russian FSB

- Developed in 2003
- Copy sensitive information of interest and then send it to Russia
- Detected on Windows, Linux and macOS computers in more than 50 countries, including Australia!
- Operations against NATO, research institutions, media organisations, financial services, government agencies and more.
- Can disrupt critical industrial control systems!

# Snake Hunting

FBI developed a PERSEUS tool to disable Snake.


Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
a part of GCHQ

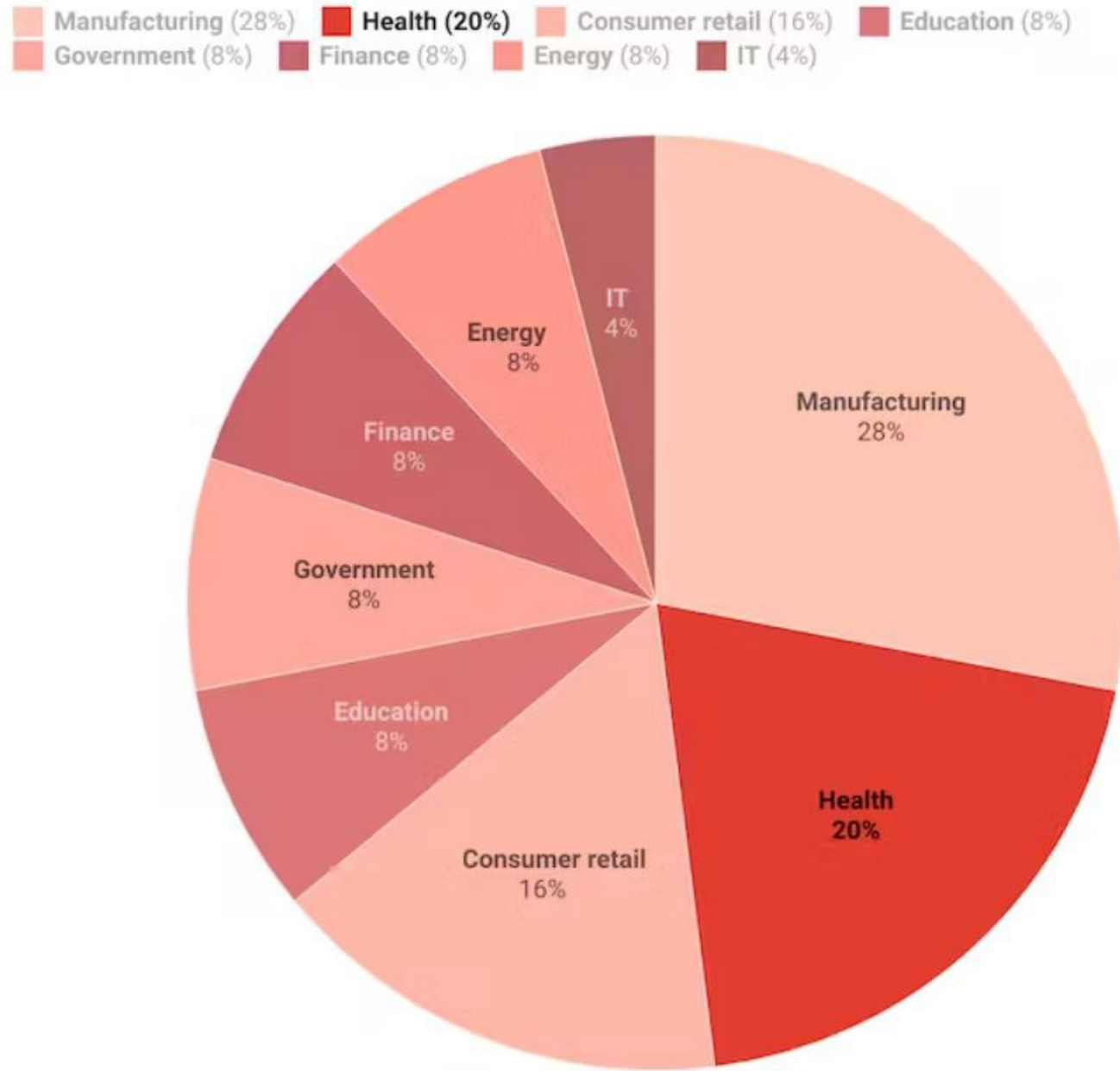
Australian Government
Australian Signals Directorate
ACSC Australian Cyber Security Centre

National Cyber Security Centre
PART OF THE GCSB

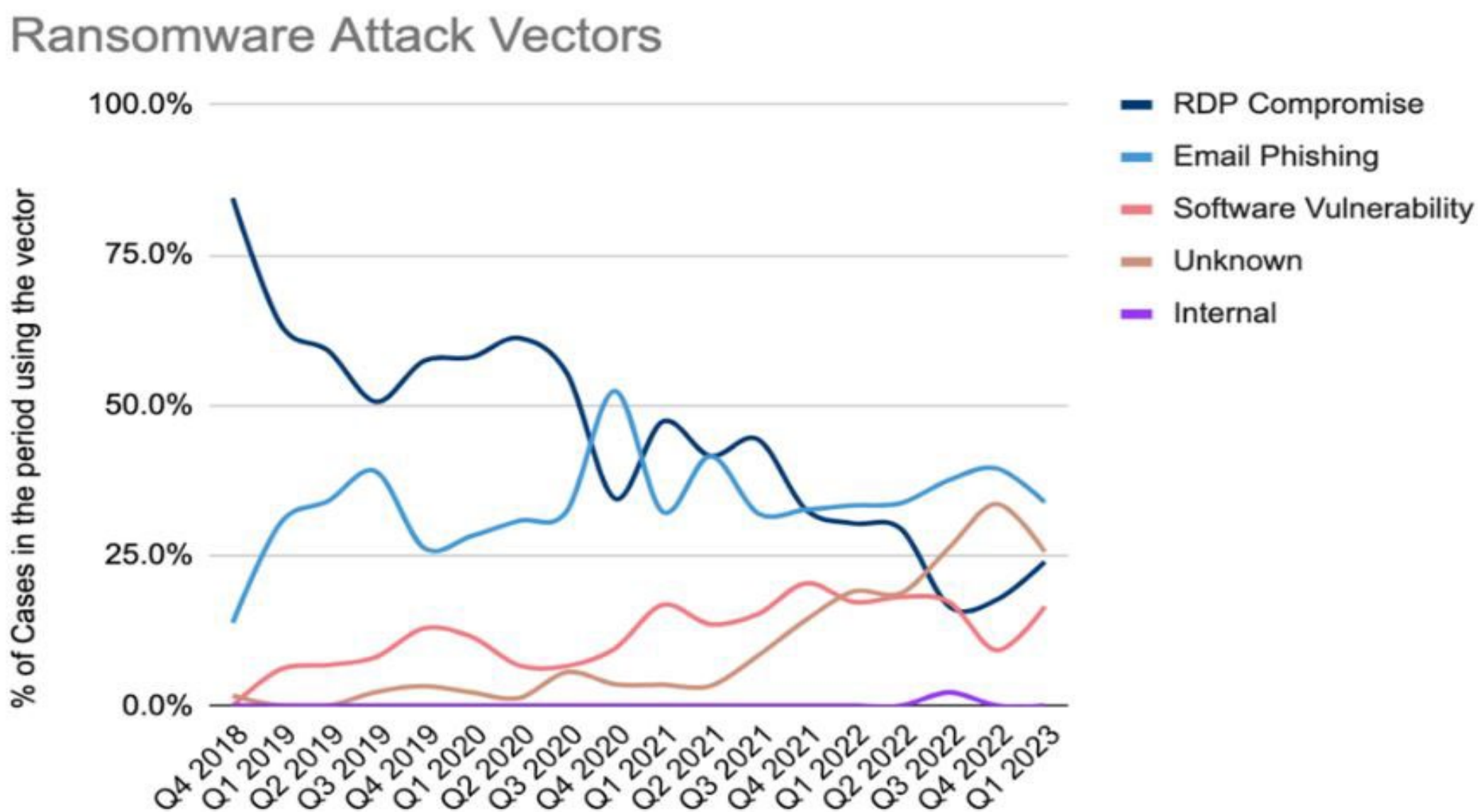
# Decentralized, Anonymous nature of Cyber Crime Economy

- ❑ Russia-Ukraine war
- ❑ Cost of living pressure

# Top targets for cyber criminals

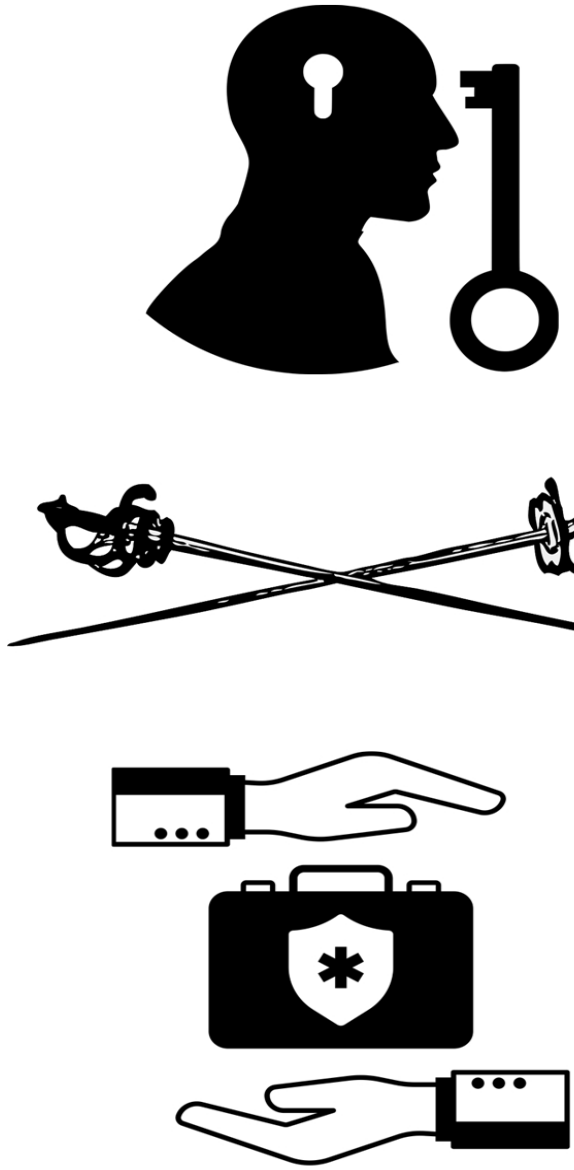



Source: Microsoft Digital Defense Report 2022 • Created with Datawrapper




Source: coveware.com

# Remedies!



- Adaptive Multi-Factor Authentication
- Covert Malware Detection
- Red-Blue Team Exercise
- Crypto De-anonymization
- Cyber Insurance

# Cyber Insurance



Business Interruption Loss

Cyber Extortion

Digital Asset Loss

Reputational Damage

Privacy Liability

- Work Integrated Learning
- Enterprise Security & Governance Projects

# Collaboration Opportunities

*"If we knew what we were doing, it wouldn't be called research, would it?"*

***– Albert Einstein***

Government of **Western Australia**
Department of **Finance**

# Please welcome

**Mr John Edwards**

**Director Cyber Security**

Office of Digital Government

# Office of Digital Government Cyber Security Unit

Cyber Risk Considerations in Procurement

# Office of Digital Government – Cyber Security Unit (CSU)

Established 2018 in the Department of the Premier and Cabinet's Office of Digital Government.

The CSU leads, coordinates and supports whole-of-government cyber security efforts to protect the WA Government's information, assets and service delivery from cyber threats.

## Responsibilities:

- Coordinating and supporting improvements to cyber security resilience across the Government Sector
- Improving visibility of cyber security threats, vulnerabilities and controls across the Government Sector
- Coordinating inter-agency operational responses to cyber security incidents
- Leading the State's inter-jurisdictional cyber security engagement
- Providing cyber security advice to Government

# WA Govt. Cyber Security Policy

## S 2. Identify

- Purpose is to develop an organisation's understanding to enable it to more effectively and efficiently manage its cyber security risks.

## S 2.1 Cyber Security Context

- Each organisation must establish its cyber security context to inform its cyber security decision-making. Organisations must
  - S2.1.F - identify suppliers and third-party partners of information systems, components and services.
- **S 2.2 Risk Assessment – The risk assessment must take account of:**
  - cyber-related supply chain risks

# WA Govt. Cyber Security Policy

- **S 3. Protect**
  - Purpose is to develop and implement appropriate safeguards to ensure delivery of critical services and protect information.
- **S 3.4 Secure Software Development**
  - Each organisation must consider security in its software development, implementation and maintenance processes for traditional, mobile and web applications.

# WA Govt. Cyber Security Policy

- **S 3.7 Secure Procurement Practices**

  Each organisation must incorporate cyber security requirements in its procurement practices for all digital goods including internet-of-things devices and services. This includes:

  a) standard cyber security clauses in all new and extended IT contracts that, among other things, require third-party service providers to report cyber security incidents to the organisation;
  b) new whole-of-government contracts applying the requirements of this Policy;
  c) developing and implementing a cyber supply chain risk management approach that is informed by the ACSC's Cyber Supply Chain Guidance prior to undertaking the procurement process;
  d) undertaking adequate due diligence on suppliers' IT controls, processes and standards to address cyber related risks at the time of contract formation and management; and
  e) the assessment of cyber risks in any contract risk assessments

# Case Study – HWLE Data Breach

- HWL Ebsworth – Australian legal service provider with a large presence in State and Federal Departments.
- 2.4 Million Documents exfiltrated from their network.
- Official Sensitive
  - Legal Professional Privilege.
  - Personally Identifiable Information.

# Case Study – Tasmanian Govt. Data Breach

- Tasmanian Education Dept. contracted services with a small service provider.
- Provided “keys” to system to automate data transfers.
- Service Provider subcontracted some work to a small TP service provider and transferred “keys”.
- TP service provider hacked.

- 16,000 documents exfiltrated.
- Personally identifiable information, including names, addresses, email, and some bank account details.

# Cyber Risk – Initial Steps.

- Establish the risk context.
  - Business impact.
    - Confidentiality – Official v's Official Sensitive
    - Integrity – Accurate, reliable
    - Availability – ensure access when required.

  - The greater the potential business impact more in depth an assessment of the providers cyber maturity will be required.
    - Low business impact e.g. non-critical service and/or only Official workloads – Self assessment/attestation.
    - High business impact e.g. critical service and/or Official Sensitive workloads – Independent security assessment against industry standards (ISO 27000, SOC2, IRAP…)

# ACSC Supply Chain Risk Management

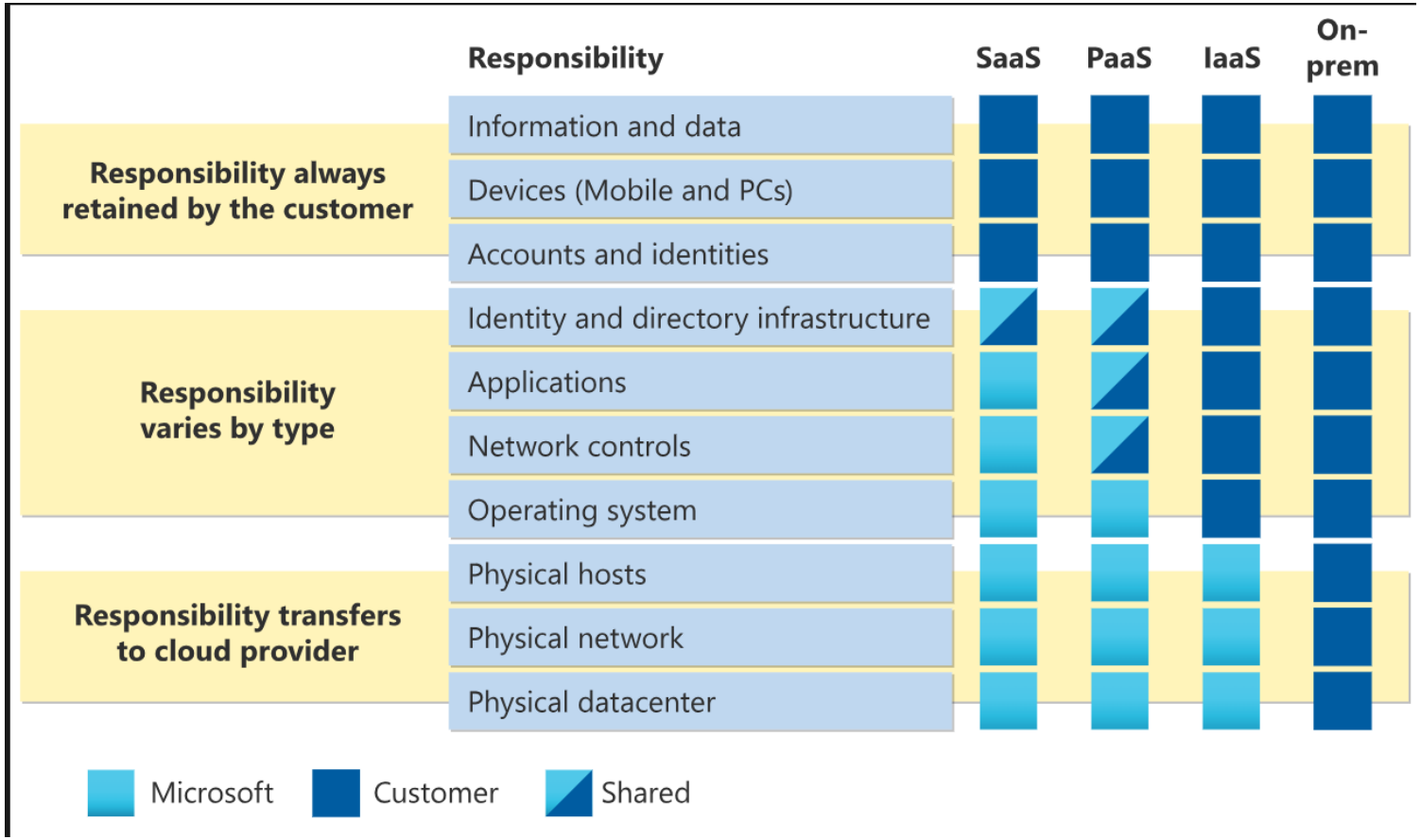
- **Set cyber security expectations**
  - cyber security expectations should be clearly documented in contracts or memorandum of understandings
  - stipulate the requirement for any cyber security incidents to be openly and transparently reported to their customers and appropriate authorities.
- **Audit for compliance**
  - routine audits or other forms of technical assessments.

- In depth guidance: https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/outsourcing-and-procurement/cyber-supply-chains/cyber-supply-chain-risk-management

# ACSC – Procurement and Outsourcing

- Assessment of Managed Service Providers
  - ***Control: ISM-1793; Revision: 0; Updated: Sep-22; Applicability: All; Essential Eight: N/A***
    *Managed service providers and their managed services undergo a security assessment by an IRAP assessor at least every 24 months.*
    - *DGov – if IRAP not available seek other assurance – ISO 27000, SOC2.*
- *Outsourced Cloud Services*
  - ***Control: ISM-1570; Revision: 1; Updated: Jun-22; Applicability: All; Essential Eight: N/A***
    *Outsourced cloud service providers and their cloud services undergo a security assessment by an IRAP assessor at least every 24 months.*
    - *DGov – if IRAP not available seek other assurance – ISO 27000, SOC2.*
- *In depth guidance : https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-procurement-and-outsourcing*

# Cloud Services Shared Responsibility Model



# Assistance

- DGov CSU – cyber.policy@dpc.wa.gov.au
- Insurance Commission of WA.

# Questions?

Government of **Western Australia**
Department of **Finance**

# We value your feedback – please take a few minutes to complete this survey