

The Evolution of Cyber Threats in the Retail Industry

© 2023 Mastercard International Incorporated. All rights reserved.
Mastercard proprietary and confidential. This presentation may not be reproduced or distributed, in whole or in part, without the prior written consent of Mastercard.



With you today...



Mallika Sathi

Vice President, Product Management
Mastercard Cyber & Intelligence



Fred Yap

Director, Advisors Client Services
Mastercard Data & Services

Setting the context



Covid-19 has forced retailers to digitise their store fronts into e-commerce platforms to meet consumer needs.



9.4 million Australian households shopped online in 2022, **spending \$63.8 billion on online goods**, contributing over 18 per cent of all retail sales.



The rise of online shopping has made customer data more valuable than ever. This data is a goldmine for attackers, who can use it to commit fraud, steal identities, and launch cyberattacks.



Data breaches are impacting businesses..

88%

of **data breaches** between July to December 2022 contained **contact information**

\$4.2M

average **cost of a data breach** in Australia



Financial gain is the primary motivation why threat actors commit **data breaches**

...and affects consumer confidence & trust

70%

of respondents believe that **companies they do business with protect their data**

up to 10M

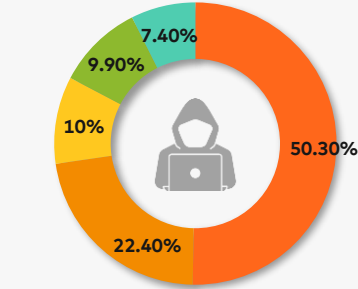
Australians were affected by data breaches between July to December 2022

up to 17% ↓

decline on card-on-file and e-commerce transactions when news of major data breaches were made public

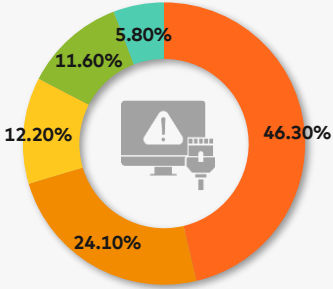
Australian retail sector threat landscape: Key threat actors, TTPs, and assets targeted

Top Threat Actors



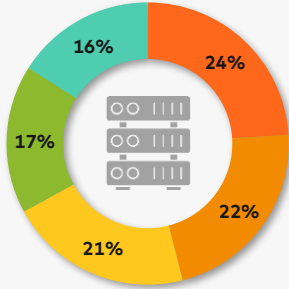
- Black Hat
- Organised Crime Group
- Unskilled Hackers
- State Sponsored Attackers
- Cyber Warriors

Top Attack Tactics, Techniques and Procedures



- Malicious Software
- Ransomware
- Information Gathering
- Phishing
- Denial of Service

Top Assets Targeted



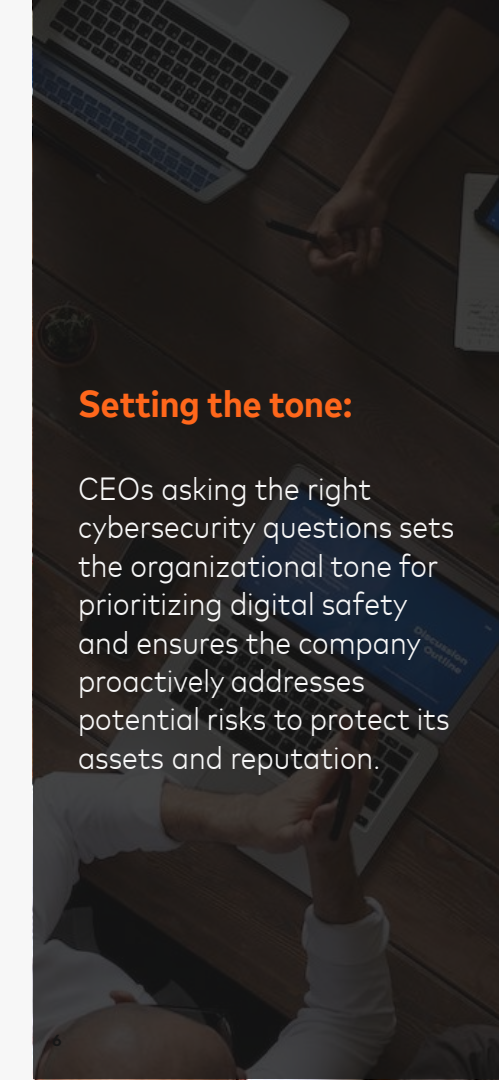
- Physical Assets
- Business Systems
- Customer Financial Information
- Customer Personal Information
- Intellectual Properties

Note: Tactics, Techniques, and Procedures (TTPs) are patterns of activities or methods associated with a specific threat actor or group of threat actors.



External and internal cyber threats targeting the Australian retail industry





Setting the tone:

CEOs asking the right cybersecurity questions sets the organizational tone for prioritizing digital safety and ensures the company proactively addresses potential risks to protect its assets and reputation.

Retail CEOs need to develop a much deeper understanding of cyber security and ask questions accordingly

01.

Are our **senior executives and board of directors onboard in our cyber security journey?**

02.

Do we have a **comprehensive view of** what are the most valuable, vulnerable and threatened **assets that must be protected?**

03.

Do we have the **right capabilities to detect and protect** against a cyber breach and are we sufficiently **prepared to respond to, and recover from a cyber attack?**

04.

Do we have a **comprehensive security awareness** program in-place **to educate and empower our staff** to identify and respond to potential security incidents?

05.

Do we have visibility of the **cyber and technology risks** introduced **by our third-party** vendors and partners, especially those that handle our sensitive information?

Achieving cyber resilience: Recommendations for CEOs



Formulate a **strategy**
to combat cyber
threats



Implement a **data
protection** program



Practise good **cyber
hygiene**



Monitor and manage
third-party risk



Invest in **people**



Stress test cyber
security controls



Build and test a
response plan



Collaborate with
industry groups

Strong cyber commitment as a business enabler:

As consumers become increasingly concerned security and protection of their data, strong cybersecurity can be a brand differentiator, as seen in industries like banking, insurance, and technology.

Questions & Answers