Cybercrime reporting in Australia

Organization	Description
ACORN	A platform that allows people to report cybercrimes such as identity theft, internet fraud, and hacking. offers guidance on reaction and prevention.
Scam Watch	Under the supervision of the Australian Competition and Consumer Commision (ACCC), it offers guidance on identifying, evading, and reporting fraudulent activities.
AFP	National legal enforcement organization that looks into and fights cybercrime, including cyberattacks and the exploitation of minors online.
AusCERT	The premier computer emergency response team in Australia, offering its members incident response and cybersecurity guidance.
ACIC	National organization in charge of criminal intelligence, emphasizing organized and serious crime, including cybercrime.
ACSC	Initiative by the government to strengthen cybersecurity across the country, offer guidance, and address cyberthreats.

Analysis of Threat Report

a.

Covid-19 themed malicious activity - Cyberthreats that take advantage of the COVID-19 epidemic include malware that spreads under the pretense of health information, phishing emails, and phony websites.

Ransomeware - malicious software that encrypts a victim's data and requests a ransom to unlock it.

Exploitation of security vulnerability - Cyberattacks that take use of holes in hardware or software to obtain access without authorization or to do harm.

Software supply chain compromises - attacks aimed at infecting legitimate apps with malicious malware by targeting software developers and suppliers.

Business email compromises - a particular kind of scam where fraudsters use hacked company email accounts to make illicit payments, specifically aimed at wire transfer businesses.

b.

Threats	Protection Approaches	Generic/Specific
COVID-19 themed malicious activity	User education and awareness	Generic
	Implementing email filtering and web security	Specific
Ransomeware	Regular Backups	Generic
	Keeping software up-to-date	Generic
	Network segmentation	Specific
Exploitation of security vulnerability	Regular patching and updates	Generic
	Conducting vulnerability assessments	Specific
Software supply chain compromises	Code review and secure coding practises	Specific
	Using trusted suppliers	generic
Business email compromises	Multi-factor authentication	Generic
	Emplotee training on phishing attacks	specific

c.

Top 3 cybercrime types reported via ReportCyber

Types of individual cybercrime

- Identity fraud – 30%
- Online banking fraud – 18%
- Online shopping fraud – 15%

Types of business cybercrime

- Email compromise – 17%
- Business email compromise fraud – 13%
- Online banking fraud – 10&

Cyber security incidents by the top 5 reporting sectors

- Federal government – 30.7%
- State and local government – 12.9%
- Professional, scientific and technical services – 6.9%
- Educational and training – 6.7%
- Healthcare and social assistance – 5.9%

Analysis of Crime Statistics

Crimes Related to Digital Forensics:

- **Cybercrime:** consists of identity theft, internet fraud, and hacking.
- **Material intended for child exploitation:** Crimes pertaining to the creation, dissemination, and acquisition of illicit materials.
- **Unauthorised access to computer data:** Cybersecurity breaches resulting in unauthorized access to computer data.
- **Digital fraud:** This includes financial fraud, phishing, and online frauds.

Trends Over the Past Decade:

- **An increase in cybercrime:** this has been observed, which is consistent with the expanding digital footprint.
- **Cases of Child Exploitation:** Considerable work has gone into tracking and prosecuting cases of child exploitation on the internet.
- **Financial Fraud:** With the growth of digital banking, there has been a notable increase in online financial fraud and scams.
- **Data Breaches:** Both individuals and organizations are being impacted by an increasing number of data breaches.

Evaluation of Case Studies

Mark Lundy Case

Conviction: Mark Lundy was found guilty of killing both his wife and daughter. The conviction was influenced by digital evidence.

NZ Police explanation: The NZ police proposed the potential of remote access or staged activities to deceive investigators in order to explain the timing mismatch (murder at 7pm, PC shutdown at 11pm). The locations and alibi of Lundy have been debunked by forensic evidence and data analysis from computers and cell phones.

Bobbie Jo Stinnett and Lisa Montgomery Case

Conviction of Lisa Montgomery: Because Lisa Montgomery killed Bobbie Jo Stinnett, she received a death sentence. Internet interactions and searches were examples of digital evidence that was very important to the investigation.

Type of Digital Evidence: The actions and intents of Montgomery were tracked through emails, search histories on the internet, and other digital imprints.

Help from Overseas Forensic Experts: Yes, to ensure a complete and accurate investigation, the FBI enlisted the help of foreign cybercrime experts to assess the digital data.