INFS 5115 Security Principles

Cybersecurity Attacks: Lifecycle and Motivations

University of South Australia

School of Information Technology and Mathematical Sciences

Cybersecurity Attacks: Lifecycle and Motivations

- In this seminar we will discuss some of the sources, methods and reasons for cybersecurity attacks.
- We will review current trends related to cybersecurity threats and will examine models of attack lifecycles that can be used to characterise cybersecurity attacks.

Cyber incident - Definition

A single event or a series of events that threatens the integrity, availability or confidentiality of digital information.

Commonwealth of Australia 2020, Australia's Cyber Security Strategy 2020, pp.11

Cyber incidents

- Suspicious system and network activities
- Compromise of sensitive information
- Unauthorised access or attempts to access a system
- Emails with suspicious attachments or links
- Denial-of-service attacks
- Suspected tampering of electronic devices

Australian Signals Directorate 2020, Preparing for and Responding to Cyber Security Incidents Viewed 17/3/21 https://www.cyber.gov.au/sites/default/files/2020-06/PROTECT%20-%20Preparing%20for%20and%20Responding%20to%20Cyber%20Security%20Incidents%20%28June%202020%29.pdf

Threats originate from various actors

Different origins are characterised by different motivations and possible consequences.

- Hacker, cracker
- Computer criminal
- Terrorist
- Industrial espionage
- Insiders

Standards Australia 2011, *Information technology—Security techniques—Information security risk management.* ISO/IEC 27005:2011, MOD, Sydney, NSW.

Malicious cyber actors

Different origins are characterised by different motivations and possible consequences.

- **Nation states and state-sponsored actors -** seek to compromise networks to obtain economic, policy, legal, defence and security information for their advantage.
- **Financially motivated criminals** - exploit and access systems for financial gain, posing a substantial threat to the economy. Transnational cyber crime syndicates, develop, share, sell and use sophisticated cyber tools and techniques.

Commonwealth of Australia 2020, Australia's Cyber Security Strategy 2020

Malicious cyber actors

- **Issue-motivated groups and individuals** - primarily concerned with drawing attention to their causes, generally less capable and less sophisticated, but still able to cause significant disruption to industry and governments.
- **Terrorist groups and extremists** - effective at using the internet to communicate and generate attention, but generally employ very basic cyber techniques and capabilities such as distributed denial of service (DDoS) activities, hijacking social media accounts and defacing websites.

Commonwealth of Australia 2020, Australia's Cyber Security Strategy 2020

Cybercrime Definition

- Crimes directed at computers or other information communications technologies (ICTs) (such as computer intrusions and denial of service attacks), and
- Crimes where computers or ICTs are an integral part of an offence (such as online fraud)

Australian Federal Police, 2021 What is Cybercrime? Viewed 16/3/21
https://www.afp.gov.au/what-we-do/crime-types/cyber-crime

Cybercrime Categories

- **Cyber abuse** – someone is bullying, harassing or stalking you online.
- **Online Image Abuse** – someone has shared online, or is threatening to share online, intimate images or videos of you.
- **Online shopping fraud or romance fraud** - you have been deceived into sending money or goods to someone online.
- **Identity theft** - someone has used your personal or business identity information and accessed your online accounts.

Australian Cyber Security Centre, 2020, ACSC Annual Cyber Threat Report July 2019 to June 2020, Commonwealth of Australia, Viewed 17/3/21 https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

Cybercrime Categories

- **Email Compromise** - you received an email containing fraudulent information that deceived you and led you to send money.
- **Internet fraud** - you clicked on a phishing link or gave someone remote access to a computer or device, and money may have been taken from your account(s).
- **Ransomware or malware** - your system or devices have been compromised and someone may be demanding money.

Australian Cyber Security Centre, 2020, ACSC Annual Cyber Threat Report July 2019 to June 2020, Commonwealth of Australia, Viewed 17/3/21
https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

Categorising Cybercriminals

- Criminals Who Use the Net As a Tool of the Crime
  - White-collar criminals
  - Computer Con Artists
  - Hackers, Crackers, and Network Attackers

- Criminals Who Use the Net Incidentally to the Crime
  - Criminals Who Use the Net to Find Victims
  - Criminals Who Use Computers or Networks for Recordkeeping
  - Criminals Who Use E-mail or Chat Services to Correspond with Accomplices

Shinder, DL & Cross, M 2008, *Scene of the Cybercrime,* 2nd edn, Syngress, Burlington.

Cybercriminals - Misconceptions

- All cybercriminals are “nerds”—bright but socially inept
- All cybercriminals have very high IQs and a great deal of technical knowledge
- All cybercriminals are male, usually teenage boys
- All teenage boys with computers are dangerous cybercriminals
- Cybercriminals aren’t “real” criminals because they don’t operate in the “real world”
- Cybercriminals are never violent
- All cybercriminals neatly fit one profile

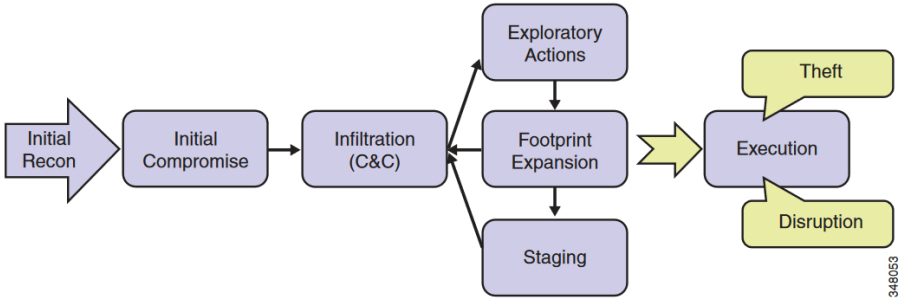
Shinder, DL & Cross, M 2008, *Scene of the Cybercrime,* 2nd edn, Syngress, Burlington.

Attack lifecycle, techniques and models

Activity :Travelex case

Summarise the steps that the perpetrators took in this case study.

Attack Lifecycle (Cisco)

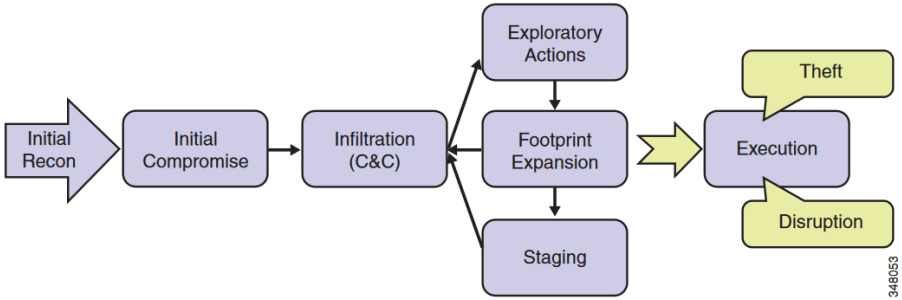


Source: https://www.cisco.com/c/dam/en/us/td/docs/security/network_security/ctd/ctd2-0/design_guides/ctd_2-0_cvd_guide_jul15.pdf

- Exploratory Actions
  - Locate resources relevant to the attacker (e.g., via scanning).
- Footprint Expansion
  - Expand from a single to multiple points of presence.
- Staging
  - Prepare for execution (dependent on attackers' goal).

Cisco 2005, 'Cisco Cyber Threat Defense v2.0: Design Guide, Cisco, viewed 23 June 2017, https://www.cisco.com/c/dam/en/us/td/docs/security/network_security/ctd/ctd2-0/design_guides/ctd_2-0_cvd_guide_jul15.pdf

Attack Lifecycle (Cisco)



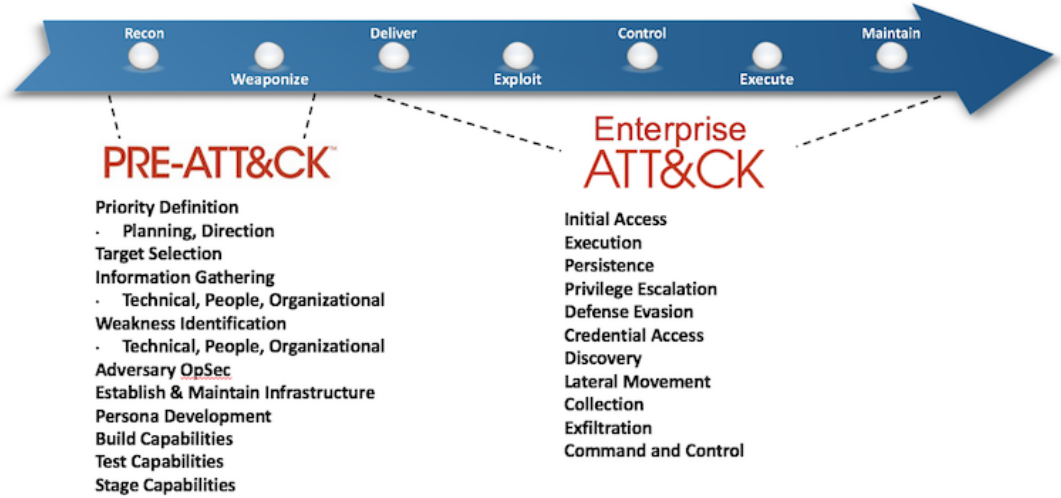
Source: https://www.cisco.com/c/dam/en/us/td/docs/security/network_security/ctd/ctd2-0/design_guides/ctd_2-0_cvd_guide_jul15.pdf

- Execution
  - Where the attacker determines their goals and objectives have been met.
  - Generally, either disruption of activities or theft of data.

Cisco 2005, 'Cisco Cyber Threat Defense v2.0: Design Guide, Cisco, viewed 23 June 2017, https://www.cisco.com/c/dam/en/us/td/docs/security/network_security/ctd/ctd2-0/design_guides/ctd_2-0_cvd_guide_jul15.pdf

MITRE ATT&CK

Knowledge base of **adversary tactics and techniques** based on real-world observations



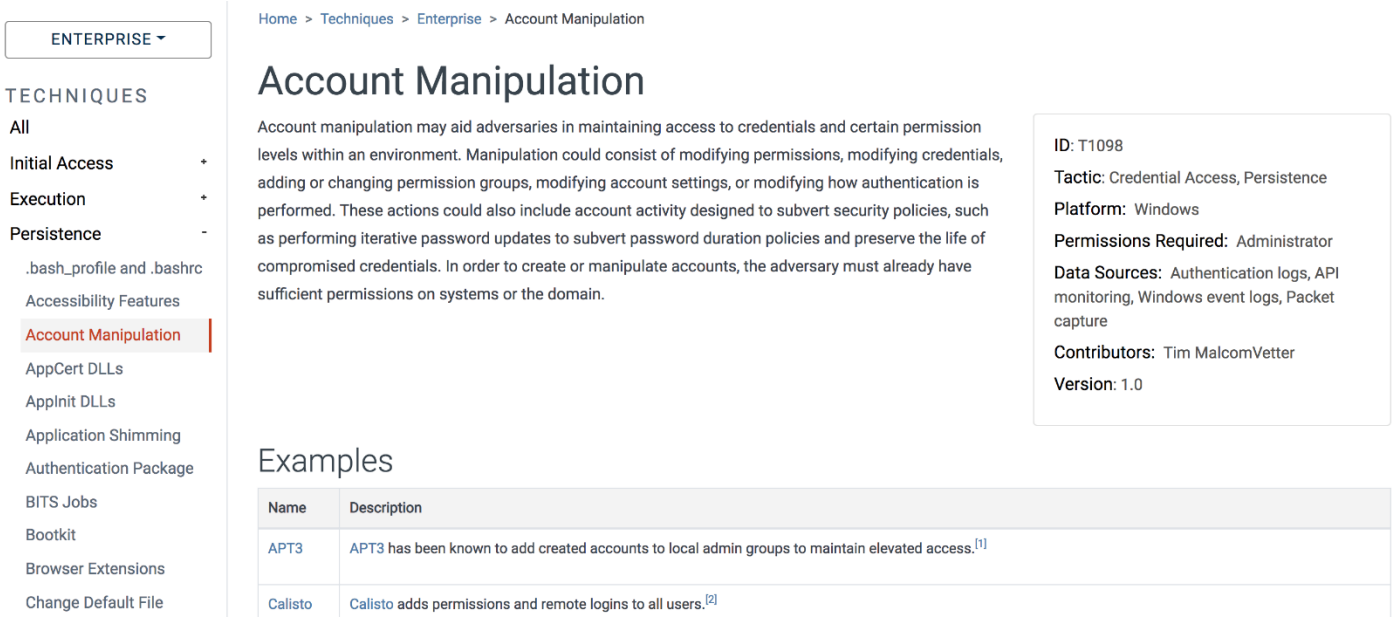
MITRE 2019, *ATT&CK*, The MITRE Corporation, https://attack.mitre.org/

MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and	Data Encoding

MITRE 2019, *ATT&CK*, The MITRE Corporation, https://attack.mitre.org/

MITRE ATT&CK Technique Example



MITRE 2019, *ATT&CK*, The MITRE Corporation, https://attack.mitre.org/

The Australian cyber threat landscape

- What is the annual Australian Cyber Security Centre (ACSC) Threat Report?
- Why is this relevant?
- How often is it published?

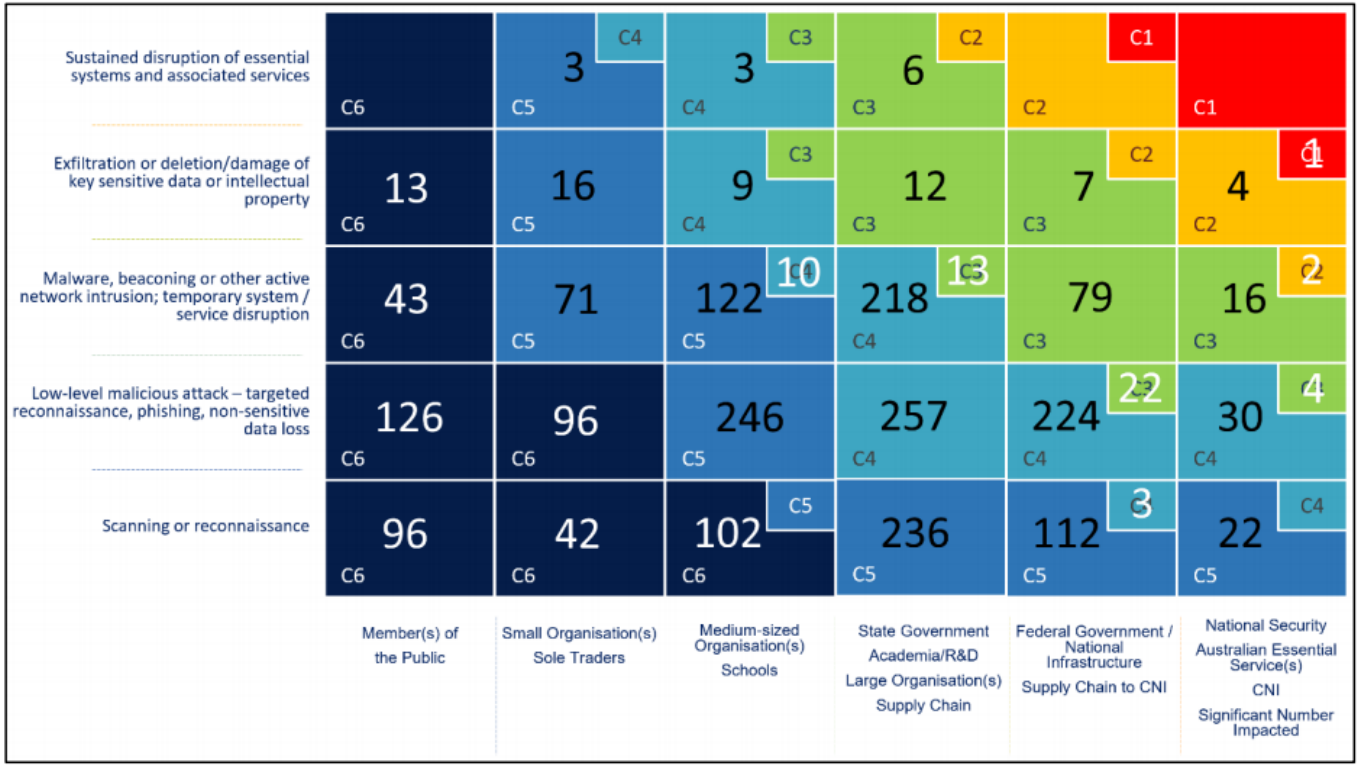
ACSC Cyber Threat Report - Jul 2019 to Jun 2020

- The annual Australian Cyber Security Centre Threat Report outlines key cyber threats and statistics over the period 1 July 2019 to 30 June 2020.

- Over this period, the ACSC responded to 2,266 cyber security incidents and received 59,806 cybercrime reports at an average of 164 cybercrime reports per day, or one report every 10 minutes

Australian Cyber Security Centre, 2020, ACSC Annual Cyber Threat Report July 2019 to June 2020, Commonwealth of Australia, Viewed 17/3/21
https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

Cyber security incidents, by categorisation

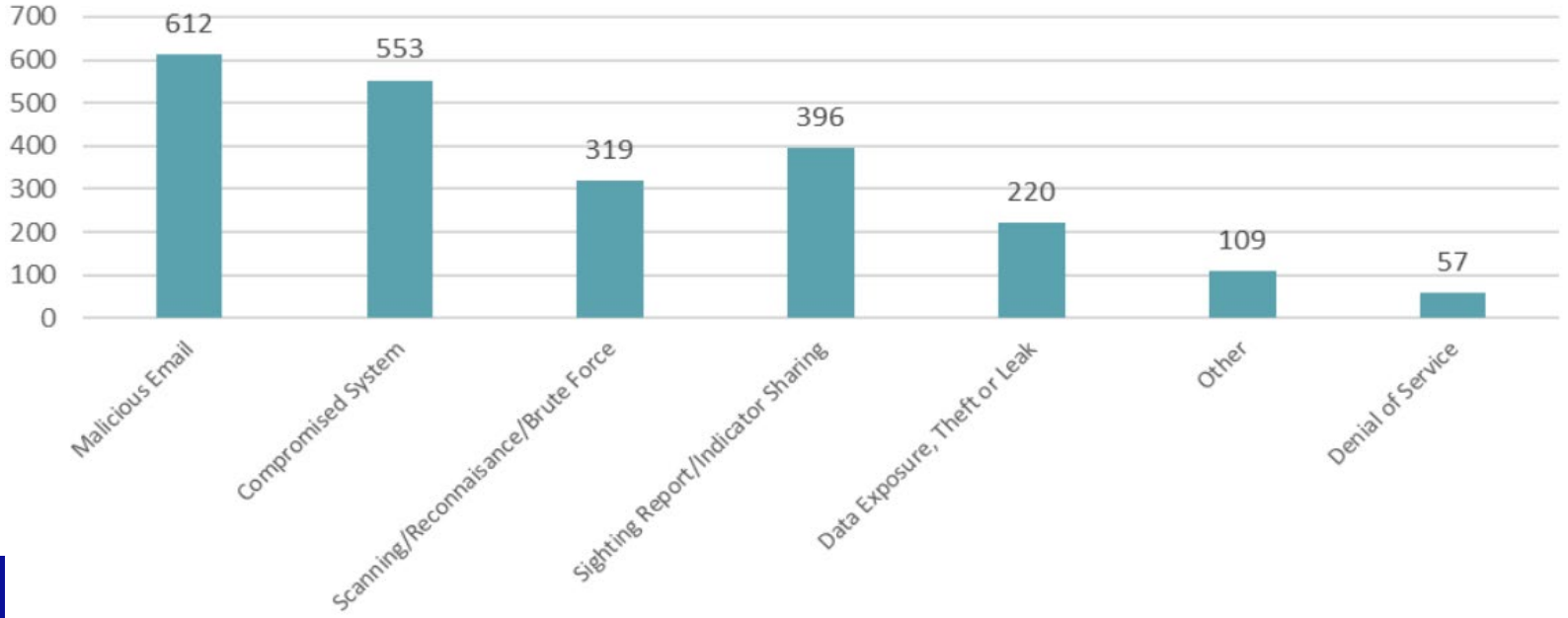


University of South Australia

School of Information Technology and Mathematical Sciences

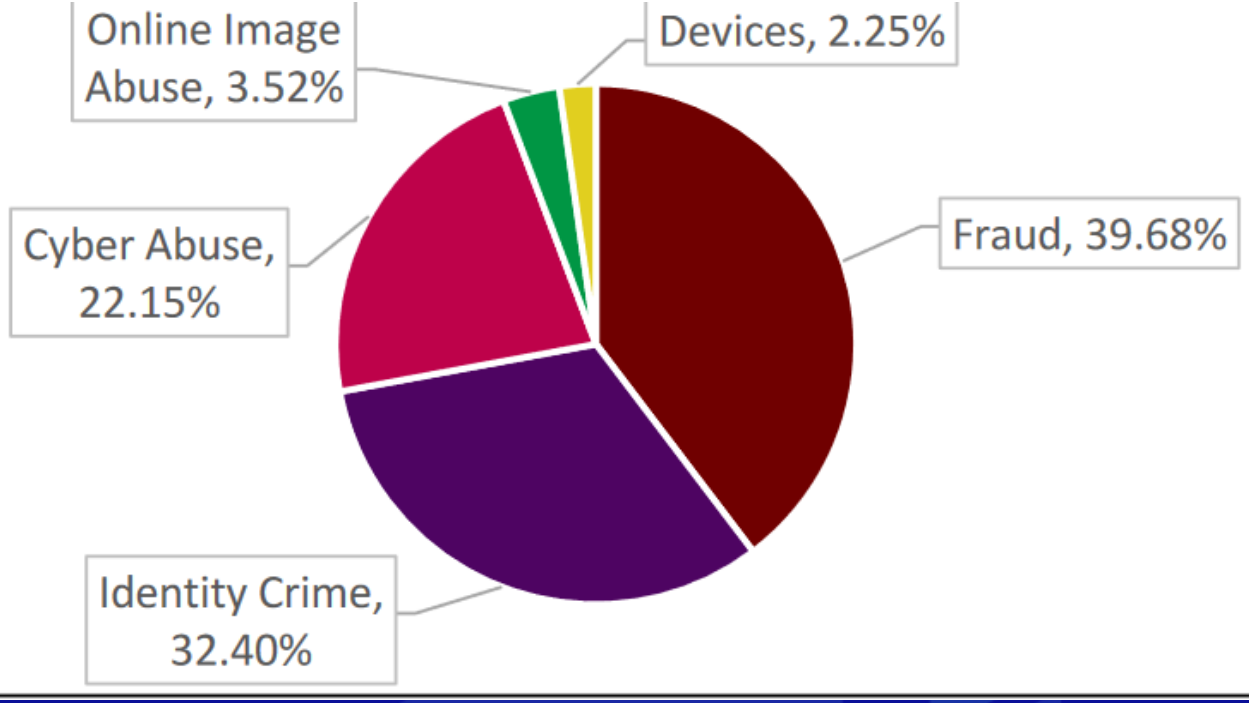
Australian Cyber Security Centre, 2020, ACSC Annual Cyber Threat Report July 2019 to June 2020, Commonwealth of Australia, Viewed 17/3/21 https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

Cyber security incidents, by type



Australian Cyber Security Centre, 2020, ACSC Annual Cyber Threat Report July 2019 to June 2020, Commonwealth of Australia, Viewed 17/3/21 https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

Cyber crime reports by categorisation



Australian Cyber Security Centre, 2020, ACSC Annual Cyber Threat Report July 2019 to June 2020, Commonwealth of Australia, Viewed 17/3/21
https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

ACSC Annual Cyber Threat Report

- Ransomware
- Phishing and Spearphishing campaigns
- Business email compromise
- Exploitation of vulnerabilities

Australian Cyber Security Centre, 2020, ACSC Annual Cyber Threat Report July 2019 to June 2020, Commonwealth of Australia, Viewed 17/3/21 https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

The global cyber threat landscape

- What/who is Verizon?
- What is their annual report and which report is this?
- Why is Verizon and their report relevant?
- How frequently does Verizon release reports?

Verizon's Data Breach Investigations Report

- A well known source of information on the changing cybersecurity threat landscape
- Based on analysis of real-world incidents
- 2020:
  - 157,525 security incidents
  - 3,950 confirmed data breaches
  - 81 contributors from international public and private entities

Verizon 2020, 2020 Data Breach Investigations Report, Verizon, Viewed 19/3/21 https://enterprise.verizon.com/en-au/resources/reports/dbir/

Verizon terminology

- ***Incident:*** *A security event that compromises the integrity, confidentiality or availability of an information asset.*

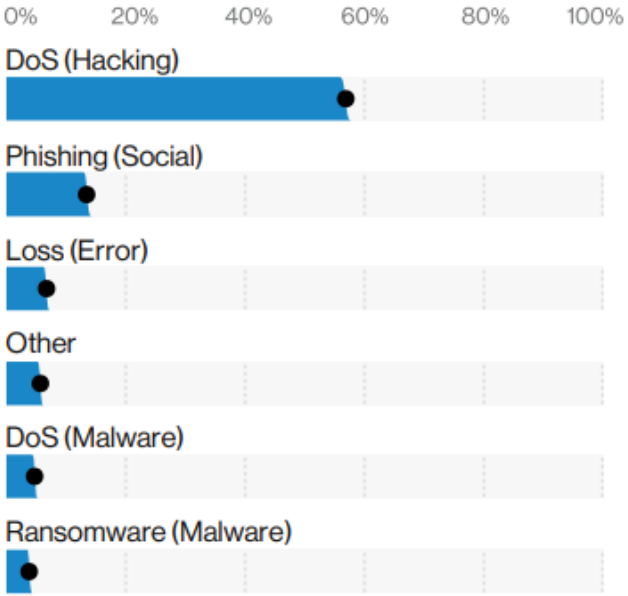
- ***Breach:*** *An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorised party.*

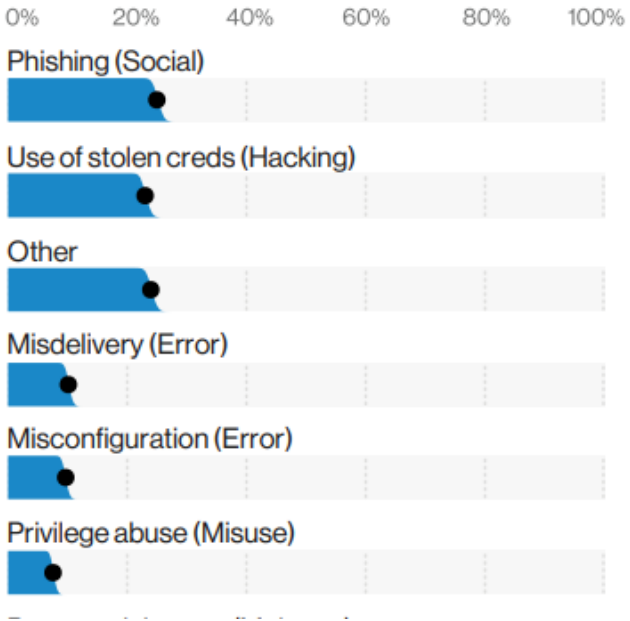
- **Threat actor:** Who is behind the event?

- **Threat action:** What tactics (actions) were used to affect an asset? Seven primary categories of threat actions: Malware, Hacking, Social, Misuse, Physical, Error and Environmental.

Verizon 2020, 2020 Data Breach Investigations Report, Verizon, Viewed 19/3/21 https://enterprise.verizon.com/en-au/resources/reports/dbir/

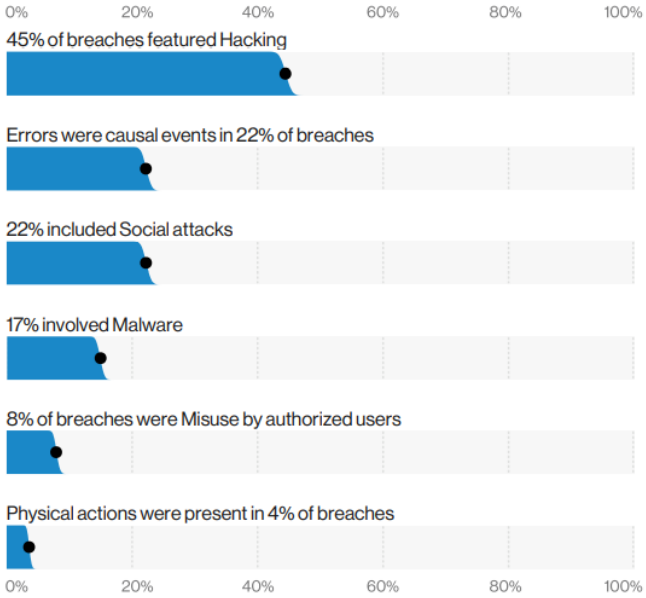
Verizon 2020 – Incidents vs Breaches

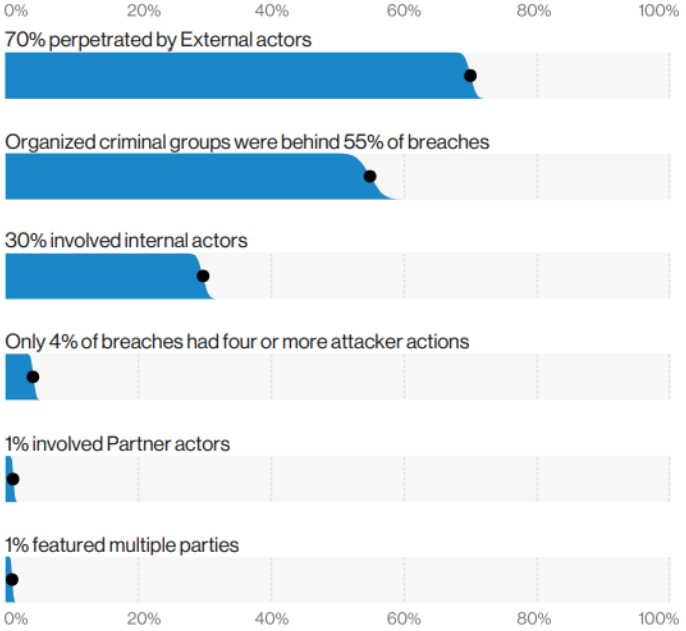




Verizon 2020, 2020 Data Breach Investigations Report, Verizon, Viewed 19/3/21 https://enterprise.verizon.com/en-au/resources/reports/dbir/

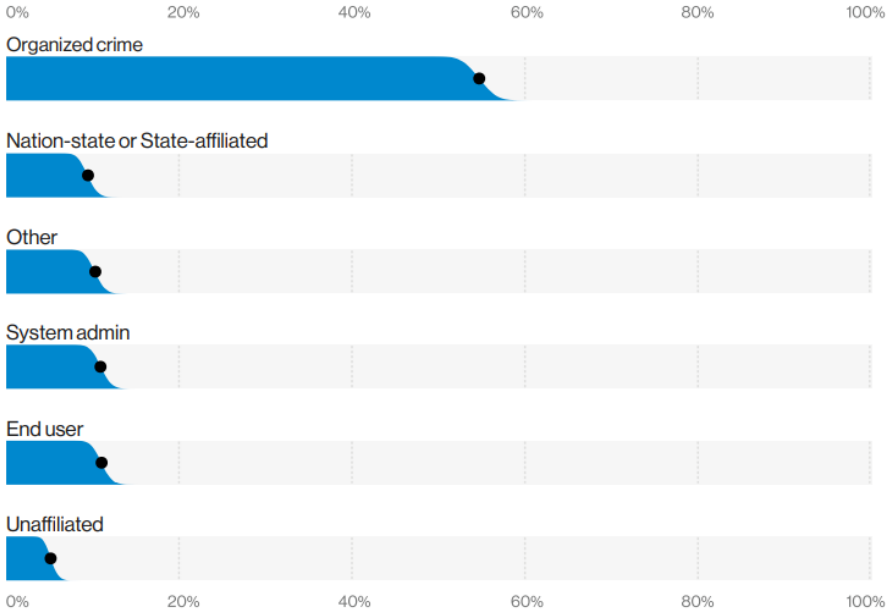
Verizon 2020 – Actions & Actors

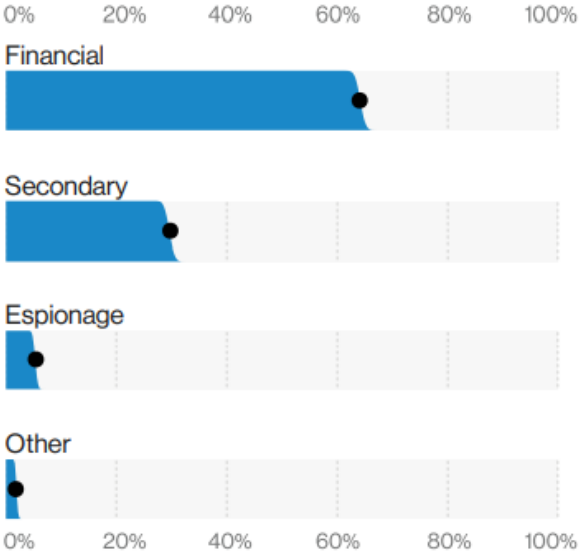




Verizon 2020, 2020 Data Breach Investigations Report, Verizon, Viewed 19/3/21 https://enterprise.verizon.com/en-au/resources/reports/dbir/

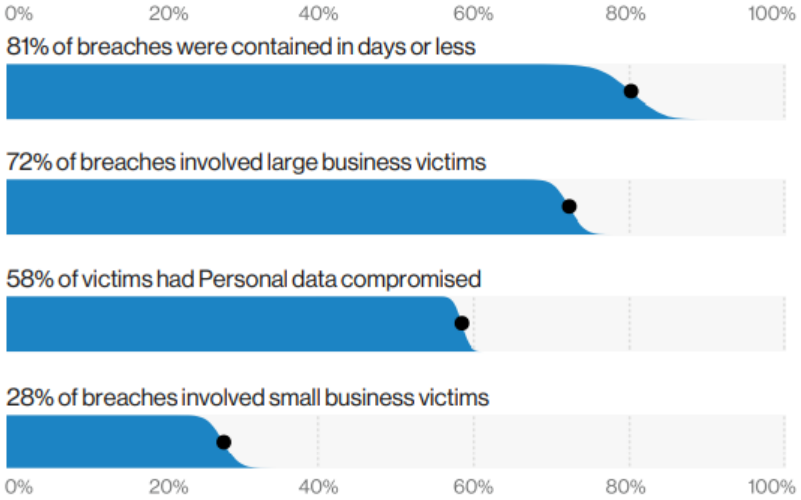
Verizon 2020 – Actors & motivation

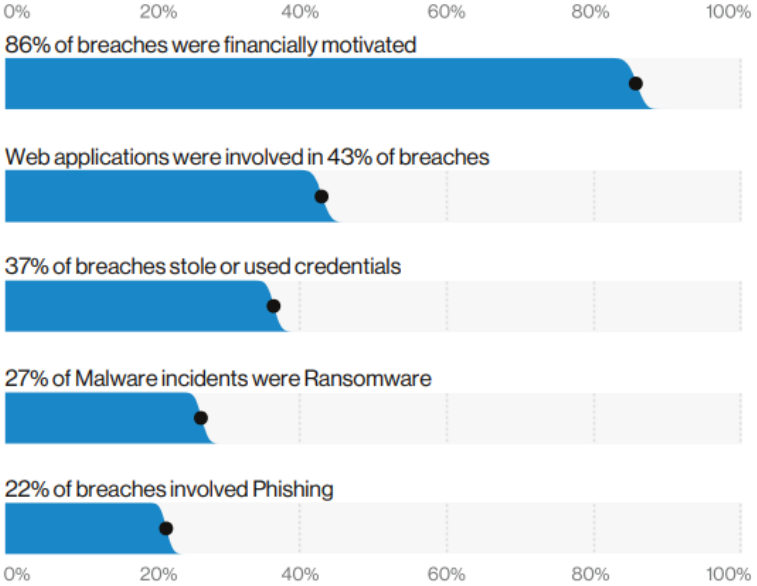




Verizon 2020, 2020 Data Breach Investigations Report, Verizon, Viewed 19/3/21 https://enterprise.verizon.com/en-au/resources/reports/dbir/

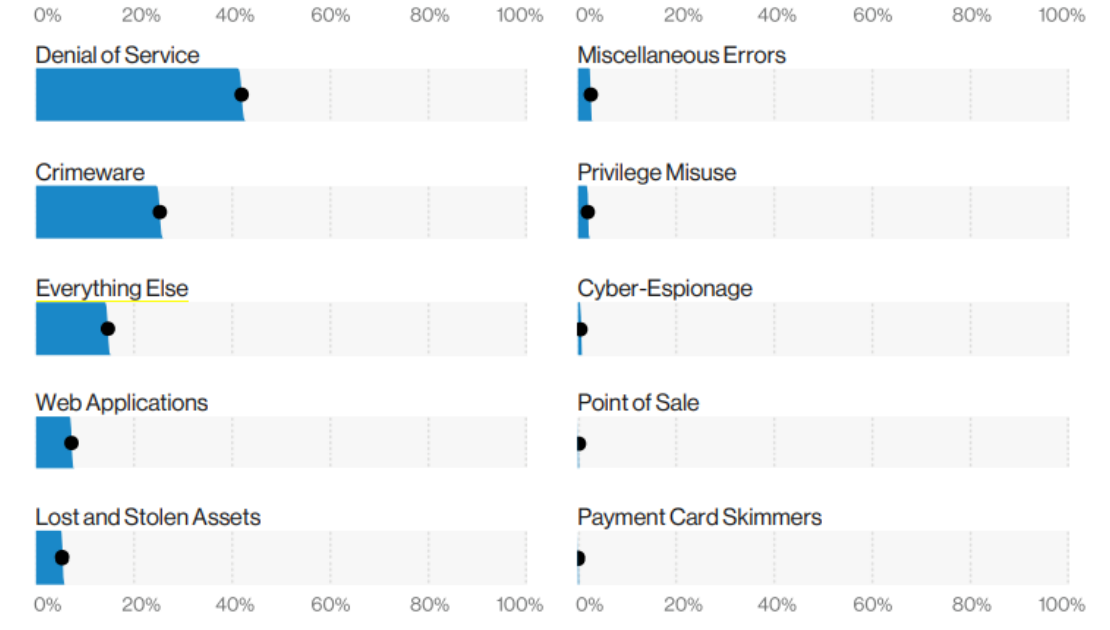
Verizon 2020 – Victims & commonalities





Verizon 2020, 2020 Data Breach Investigations Report, Verizon, Viewed 19/3/21 https://enterprise.verizon.com/en-au/resources/reports/dbir/

Verizon 2020 – Patterns



Verizon 2020, 2020 Data Breach Investigations Report, Verizon, Viewed 19/3/21 https://enterprise.verizon.com/en-au/resources/reports/dbir/

Educational Services

Phishing attacks in 28% of breaches and hacking via stolen credentials in 23% of breaches. In incident data, Ransomware accounts for approximately 80% of Malware infections in this vertical. Educational Services performed poorly in reporting phishing attacks

Top Patterns	Everything Else, Miscellaneous Errors and Web Applications represent 81% of breaches.
Threat Actors	External (67%), Internal (33%), Partner (1%), Multiple (1%) (breaches)
Actor Motives	Financial (92%), Fun (5%), Convenience (3%), Espionage (3%), Secondary (2%) (breaches)
Data Compromised	Personal (75%), Credentials (30%), Other (23%), Internal (13%) (breaches)

Verizon 2020, 2020 Data Breach Investigations Report, Verizon, Viewed 19/3/21 https://enterprise.verizon.com/en-au/resources/reports/dbir/

Financial and Insurance

Attacks perpetrated by external actors who are financially motivated to get easily monetized data (63%), internal financially motivated actors (18%) and internal actors committing errors (9%). Web Applications attacks that leverage the USE of stolen credentials also continue to affect this industry.

Top Patterns	Web Applications, Miscellaneous Errors and Everything Else represent 81% of breaches.
Threat Actors	External (64%), Internal (35%), Partner (2%), Multiple (1%) (breaches)
Actor Motives	Financial (91%), Espionage (3%), Grudge (3%) (breaches)
Data Compromised	Personal (77%), Other (35%), Credentials (35%), Bank (32%) (breaches)

Verizon 2020, 2020 Data Breach Investigations Report, Verizon, Viewed 19/3/21 https://enterprise.verizon.com/en-au/resources/reports/dbir/

Healthcare

Financially motivated criminal groups continue to target this industry via ransomware attacks. Lost and stolen assets also remain a problem. Basic human error is alive. Mis delivery was top spot among Error action types, while internal Misuse has decreased

Top Patterns	Miscellaneous Errors, Web Applications and Everything Else represent 72% of breaches.
Threat Actors	External (51%), Internal (48%), Partner (2%), Multiple (1%) (breaches)
Actor Motives	Financial (88%), Fun (4%), Convenience (3%) (breaches)
Data Compromised	Personal (77%), Medical (67%), Other (18%), Credentials (18%) (breaches)

Verizon 2020, 2020 Data Breach Investigations Report, Verizon, Viewed 19/3/21 https://enterprise.verizon.com/en-au/resources/reports/dbir/

Information

Web App attacks via vulnerability exploits and the Use of stolen credentials are prevalent in this industry. Errors continue to be a significant factor and are primarily made up of the Misconfiguration of cloud databases. Growth in Denial-of-Service attacks also remains a problem for the Information sector.

Top Patterns	Web Applications, Miscellaneous Errors and Everything Else represent 88% of data breaches.
Threat Actors	External (67%), Internal (34%), Multiple (2%), Partner (1%) (breaches)
Actor Motives	Financial (88%), Espionage (7%), Fun (2%), Grudge (2%), Other (1%) (breaches)
Data Compromised	Personal (69%), Credentials (41%), Other (34%), Internal (16%) (breaches)

Verizon 2020, 2020 Data Breach Investigations Report, Verizon, Viewed 19/3/21 https://enterprise.verizon.com/en-au/resources/reports/dbir/

Manufacturing

Manufacturing is beset by external actors using password dumper malware and stolen credentials to hack into systems and steal data. While the majority of attacks are financially motivated, Cyber-Espionage-motivated attacks are a concern as well. Internal employees misusing their access to abscond with data also remains a concern.

Top Patterns	Crimeware, Web Applications and Privilege Misuse represent 64% of breaches.
Threat Actors	External (75%), Internal (25%), Partner (1%) (breaches)
Actor Motives	Financial (73%), Espionage (27%) (breaches)
Data Compromised	Credentials (55%), Personal (49%), Other (25%), Payment (20%) (breaches)

Verizon 2020, 2020 Data Breach Investigations Report, Verizon, Viewed 19/3/21 https://enterprise.verizon.com/en-au/resources/reports/dbir/

Professional, Technical and Scientific Services

Financially motivated attackers continue to steal credentials and leverage them against web application infrastructure. Social engineering in the form of Phishing and Pretexting is a common tactic used to gain access. This industry also suffers from Denial of Service attacks regularly

Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 79% of breaches.
Threat Actors	External (75%), Internal (22%), Partner (3%), Multiple (1%) (breaches)
Actor Motives	Financial (93%), Espionage (8%), Ideology (1%) (breaches)
Data Compromised	Personal (75%), Credentials (45%), Other (32%), Internal (27%) (breaches)

Verizon 2020, 2020 Data Breach Investigations Report, Verizon, Viewed 19/3/21 https://enterprise.verizon.com/en-au/resources/reports/dbir/

Public Administration

Ransomware is a large problem for this sector, with financially motivated attackers utilizing it to target a wide array of government entities. Misdelivery and Misconfiguration errors also persist in this sector.

Top Patterns	Miscellaneous Errors, Web Applications and Everything Else represent 73% of breaches.
Threat Actors	External (59%), Internal (43%), Multiple (2%), Partner (1%) (breaches)
Actor Motives	Financial (75%), Espionage (19%), Fun (3%) (breaches)
Data Compromised	Personal (51%), Other (34%), Credentials (33%), Internal (14%) (breaches)

Verizon 2020, 2020 Data Breach Investigations Report, Verizon, Viewed 19/3/21 https://enterprise.verizon.com/en-au/resources/reports/dbir/

Retail

Attacks against e-commerce applications are the leading cause of breaches in this industry. As organizations continue to move their primary operations to the web, the criminals migrate along with them. Personal and Credentials also continue to be highly sought after in this sector.

Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 72% of breaches.
Threat Actors	External (75%), Internal (25%), Partner (1%), Multiple (1%) (breaches)
Actor Motives	Financial (99%), Espionage (1%) (breaches)
Data Compromised	Personal (49%), Payment (47%), Credentials (27%), Other (25%) (breaches)

Verizon 2020, 2020 Data Breach Investigations Report, Verizon, Viewed 19/3/21 https://enterprise.verizon.com/en-au/resources/reports/dbir/

Asia Pacific region

Targeted by financially motivated actors deploying ransomware to monetize access. Phishing (often business email compromises), internal errors and a higher-than-average Cyber-Espionage-related breaches. Web application infrastructure is being targeted both by Denial of Service attacks affecting the availability of the assets, and by hacking attacks leveraging stolen credentials.

Top Patterns	Web Applications, Everything Else and Miscellaneous Errors represent 90% of breaches.
Threat Actors	External (83%), Internal (17%), Partner (0%) (breaches)
Actor Motives	Financial (63%), Espionage (39%), Fun (4%) (breaches)
Data Compromised	Credentials (88%), Internal (14%), Other (9%), Personal (6%) (breaches)

Verizon 2020, 2020 Data Breach Investigations Report, Verizon, Viewed 19/3/21 https://enterprise.verizon.com/en-au/resources/reports/dbir/

Discussion

The Australian Cyber Security Centre (July 2019 – June 2020) threat report outlines three of the current trends as listed below:

- Malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale, and sophistication. Phishing and spearphishing remain the most common methods used by cyber adversaries to harvest personal information or user credentials to gain access to networks, or to distribute malicious content.
- Ransomware has become one of the most significant threats given the potential impact on the operations of businesses and governments. Cybercriminals often illicitly obtain user logins and credentials through spearphishing, before utilising remote desktop protocol (RDP) services to deploy ransomware on their targets.
- The 5G network and IoT devices have the potential to be revolutionary, but they require new thinking about how best to adopt them securely. Insecure or misconfigured systems make it very easy for hackers looking to compromise networks, cause harm and steal information. Specifically, the increased use of consumer IoT devices such as internet-enabled home assistants, TVs, fridges, baby monitors and home security systems will create more vulnerabilities in networks.

With the Covid-19 crisis, a lot of the employees in your organisation have had to work from home, your organisation is considering whether they should:

a) Continue to operate with most of their staff working from home, except for essential workers or

b) Continue with all employees working on site in shifts to minimise contact and potential spread of Covid-19

They have asked you to consider the cybersecurity trends outlined above and advise on whether a) it will be safer from a cybersecurity perspective to continue with employees working from home or b) continue to work with less employees at the office with reduced numbers in shifts to meet Covid-19 guidelines.

Discuss and contrast how each of these trends impact on your organisation in both scenario A and B, in addition to making a recommendation.

Australian Cyber Security Centre, 2020, ACSC Annual Cyber Threat Report July 2019 to June 2020, Commonwealth of Australia, pp. 4, Viewed 17/3/21
https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf