

# IFB240 Cyber Security

## Lecture 2 - Part A

### Threats to information & systems

Dr Leonie Simpson

[lr.simpson@qut.edu.au](mailto:lr.simpson@qut.edu.au)

# Introduction

- Information
  - is an important asset for individuals and organisations, and
  - is stored, transmitted, processed and displayed in various formats
- Information security
  - is about protecting information assets from damage or harm
- Cyber security
  - is about protecting the confidentiality, integrity and availability of digital systems, devices and the information residing on them
- Fundamental concepts in cyber/info sec: traditional goals
  - C : preventing *unauthorised* disclosure of information
  - I : preventing *unauthorised* modification or destruction of information
  - A : ensuring resources are accessible when required by an *authorised* entity

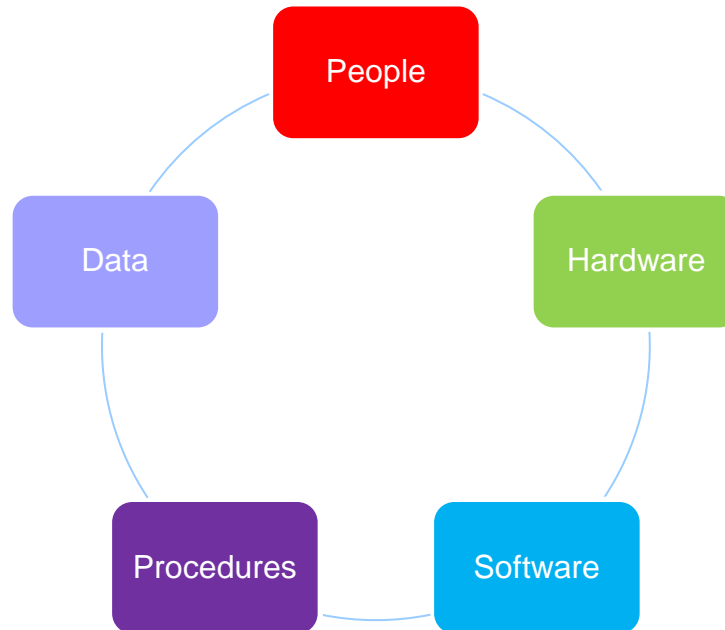
# Introduction

## Review of terminology

- Threat
  - Any circumstance or event with the potential to cause harm to an asset by compromising security goals
    - Potential cause of an undesirable event that results in harm
- Vulnerability
  - Characteristic of, or weakness in, a system that could
    - if acted on by a threat - result in harm to asset
- Security Incident
  - Occurs when threats and vulnerabilities coincide
  - Attack: when vulnerabilities are deliberately exploited

# Introduction

- Consider threats and vulnerabilities for all components of information system, and interactions between components



# Threats - Terminology

- Threat actor

- Person or entity whose actions impact *or have the potential to impact* information security
  - May be referred to as a malicious actor

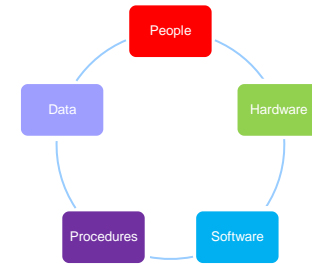
- Threat action

- What was done *or intended* to cause harm to the information asset
- Vocabulary for Event Recording and Incident Sharing (VERIS) have seven action categories
  - Error, Environmental, Hacking, Malware, Misuse, Physical, Social

# Threat actors

- Common types of threat actors & *motivations*
  - External
    - Cyber criminals - *money*
    - Hacktivist – *ideology* – *support for a cause*
    - Nation-state attackers - *political*
    - Script kiddies – *thrill seeking, bragging rights*
  - Internal
    - Careless/negligent worker – *no intention to cause harm – unaware of security impact*
    - Malicious insider – *money, or desire to disrupt*

# Threats



- Threat sources

- **External:** from outside an organisation or system

- Examples include **people** who are not authorized to use your information systems

- May need access to assets in order to cause harm
        - » Physical and/or logical access

- **Internal:** lies within the organisation or system

- Examples include **people** who are authorized to use information systems, but might use them in unauthorized manner: employees, contractors, clients, visitors, ...

- May misuse systems or exceed their authorization
      - May damage systems *accidentally*

# Threats

- Threat type
  - Natural event
    - Examples: Earthquake, Fire, Flood, Storm, Tornado, Tidal Wave, Extreme Temperature, Vermin
  - Human action
    - Accidental (no intent to cause harm)
      - Examples: Acts of negligence, errors, omissions
    - Deliberate (intended to cause harm)
      - Examples: Espionage, fraud, sabotage, theft



# Threats

- Natural events

- Potential for threat to occur may depend on physical location of the information asset
  - Historical data may be useful indicator
  - Recent examples:
    - Australia: February 2024 massive storms in Victoria
    - Turkiye and Syria: February 2023 – Earthquake
    - New Zealand: February 2023 - Cyclone
    - Australia: Brisbane: January 2022 floods
    - Australia: January 2020 – Bushfires
    - Japan: July 2018 – Floods, landslides
    - Hawaii: May 2018 - Volcano
- Most likely results in compromise of ...
  - Which goal? Think C I A

# Threats – natural events

- Example: Storms in Victoria, Australia Feb 2024
- Source: [Hundreds of Victorians remain without power after last week's storms. Some are at relief centres and unable to work - ABC News](#)

## Hundreds of Victorians remain without power after last week's centres and una

7.30 / By Rhiana Whitson and Nicole Asher  
Posted Wed 21 Feb 2024 at 6:42pm, updated

More than a week after deadly storms tore through Victoria, knocking out power to more than half a million customers, the lights are still out in some hard-hit areas of the state.

When 7.30 visited the Cockatoo relief centre in the foothills of Melbourne's Dandenong Ranges on Tuesday, thousands of households and businesses had been without power for seven days.



# STILL

# W

AusNet Services spokesperson Steven Neave apologised to customers for the time it had taken to restore power to the area. He said it was "the biggest weather event we've seen in terms of customer impacts".

AusNet is one of five electricity distribution companies in Victoria and owns wires covering about 80,000 kilometres of the state. The company also owns the state's transmission towers – six of which were destroyed in the storms last week.

There are calls for a national review of electricity security after wild storms left hundreds of thousands of households without power in Victoria. (Rhiana Whitson)

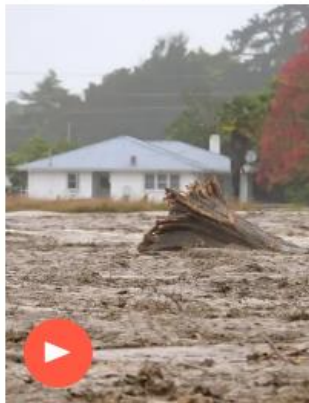
# Threats – natural events

- Example: Cyclone Gabrielle, NZ, February 2023
- [Cyclone Gabrielle worst storm to hit New Zealand this century, says PM | Cyclone Gabrielle | The Guardian](#)

## Cyclone Gabrielle worst storm to hit New Zealand this century, says PM

National state of emergency invoked and thousands displaced as storm devastates large parts of North Island and minister says 'this is climate change'

- Minister gives furious speech about 'lost decades spent bickering' over climate crisis
- Cyclone Gabrielle batters New Zealand
- Tell us: have you been affected?



Submerged truck shows dramatic rise of flood waters in New Zealand during Cyclone Gabrielle – video

New Zealand is in a national state of emergency, as Cyclone Gabrielle batters the country, with floods trapping people on roofs, thousands displaced and landslides destroying homes in what officials have described as an “unprecedented” natural disaster.

“Cyclone Gabrielle is the most significant weather event New Zealand has seen in this century. The severity and the damage that we are seeing has not been experienced in a generation,” the prime minister, Chris Hipkins, said on Tuesday. “We are still building a picture of the effects of the cyclone as it continues to unfold. But what we do know is the impact is significant and it is widespread.”

About 2,500 people have been displaced so far, officials said on Tuesday afternoon – but that number may shift, as there are still large areas that are unreachable and cut off from telecommunications.

# Threats – natural events

- Example:  
Turkiye & Syria  
earthquake
- Feb 2023
- Magnitude 7.8 quake hit  
southern Turkey and  
northern Syria, followed  
by strong aftershocks
- Source: [UN says at least 50,000  
killed in Turkey and Syria quakes | AP  
News](#)

## UN says at least 50,000 killed in Turkey and Syria quakes



People stand by a building destroyed in recent earthquake in Aleppo, Syria, Monday, Feb. 27, 2023. (AP Photo/Omar Sanadki)

BY EDITH M. LEDERER

Published 6:02 AM GMT+10, March 1, 2023

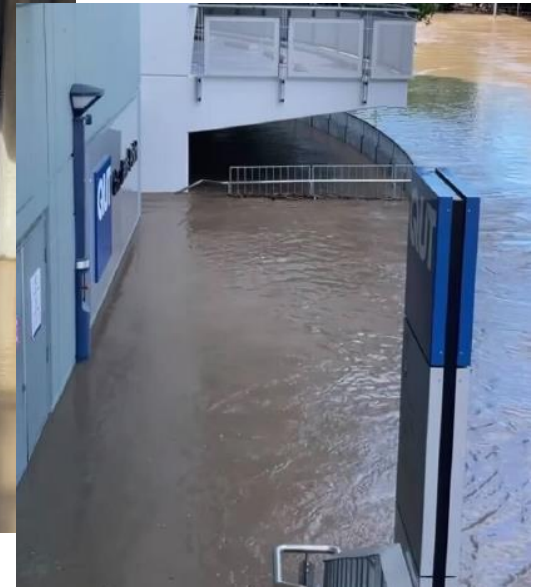
Share

UNITED NATIONS (AP) — The devastating earthquakes that struck Turkey and Syria have killed at least 50,000 people with many more injured, tens of thousands still missing and hundreds of thousands homeless, the U.N. humanitarian chief said Tuesday.



# Threats – natural events

- Example: Brisbane floods – February 2022
  - How were information systems affected in CBD? Think CIA?



[Brisbane and south-east Queensland's weekend of wild weather and flooding, in pictures - ABC News](#)

# Threats – natural events

- Example: Australian bushfires Dec 2019 - Jan 2020
- <https://www.abc.net.au/news/2020-01-01/where-and-how-the-massive-new-years-fires-hit-and-destroyed/11835740>

## **Bushfires in NSW and Victoria destroy entire towns on New Year's Eve**

By Paul Johnson

Posted 1 Jan 2020, updated 6 Jan 2020



Footage has revealed the extent of destruction in Mallacoota

# Threats

- Human action – accidental
  - No intention to cause harm, but actions do have potential for harm. Examples include
    - Accidental damage to equipment
    - Change management errors
    - Configuration errors
    - Lost property
    - Misdirecting messages
    - Operational errors (accidental deletion of files, incorrect data entry)
    - Programming errors ...
  - Consider physical and logical assets
  - Security goals compromised?
    - depends on both the accidental action and information asset

# Threats

- Example: Human action – accidental
  - <https://www.arnnet.com.au/article/642158/telstra-flags-weekend-repair-work-after-cable-cut-kills-services/>

## Telstra flags weekend repair work after cable cut kills services

The outages caused by the severed cables, which also affected some wholesale services, began on the morning of 6 June



Leon Spencer (ARN)  
08 June, 2018 15:55



0



0 Comments



The work being undertaken by Telstra to repair fibre optic cables in suburban Sydney that were accidentally cut by a third party, knocking out some broadband and ADSL services, is expected to continue into the weekend.

FOLLOW US



DISTRIBUTOR DIRECTORY

YOUR ESSENTIAL GUIDE TO AUSTRALIAN DISTRIBUTORS





# Threats

- Example: Human action – accidental
  - G20 Summit, Brisbane November 2014
  - <https://www.theguardian.com/world/2015/mar/30/personal-details-of-world-leaders-accidentally-revealed-by-g20-organisers>
  - <https://www.documentcloud.org/documents/1697616-g20-world-leaders-data-breach.html>

FOR OFFICIAL USE ONLY  
SENSITIVE

Document 1 -  
Attachment

## Step 1: Breach Containment and Preliminary Assessment

In relation to the breach, I, s 22(1) Director, Visas Services Support and Major Events Section, Department of Immigration and Citizenship, am leading the initial investigation.

An email was sent on 7 November 2014 containing the personal information, including passport details and visa status, of Leaders coming to the G20 Leaders' Summit. The purpose of the email was to advise one s 22(1) within the Department of the status of Leader's visa applications to assist in the Department's overall management of visas for the event.

s 22(1) Assistant Director, Visa Services Support and Major Events Section, accidentally sent the email to a s 22(1) who works for the Asian Cup Local Organising Committee instead of s 22(1)

This breach relates to one email and one email address.

The matter was brought to my attention directly by s 22(1) immediately after receiving an email from s 22(1) informing her that she had sent the email to the wrong person. This was less than ten minutes after the original email was sent. In his response to s 22(1), s 22(1) advised that he had deleted the email.

# Threats

- Example: Human action – accidental
  - Prince William royal photo shoot, November 2012
  - <https://grahamcluley.com/prince-william-photos-password/>



# Threats

- Human action – deliberate
  - Actions intended to cause harm to information assets
    - Examples include:
      - Eavesdropping, Espionage, Extortion, Fire, Fraud, Industrial action, Malicious code, Sabotage, Social engineering, Theft, Vandalism
  - Consider physical and logical assets
  - Possible to compromise all security goals
    - Depends on the actions taken and the asset involved
  - For the examples listed above, determine the security goal most likely to be compromised

# Threats


- Example: Human action – deliberate
- Apple former employee and theft of trade secrets
- <https://www.justice.gov/usao-ndca/pr/former-apple-employee-indicted-theft-trade-secrets>

U.S. Attorneys » Northern District of California » News

Department of Justice

U.S. Attorney's Office

Northern District of California

SHARE 

FOR IMMEDIATE RELEASE

Monday, July 16, 2018

## Former Apple Employee Indicted On Theft Of Trade Secrets

SAN JOSE - A federal grand jury in San Jose indicted Xiaolang Zhang on Thursday, July 12, 2018, for theft of trade secrets, announced Acting United States Attorney Alex G. Tse and Federal Bureau of Investigations, Special Agent in Charge John F. Bennett. Zhang was arraigned before U.S. Magistrate Judge Virginia K. DeMarchi today on charges of theft of trade secrets, in violation of 18 U.S.C. § 1832. Zhang entered a plea of not guilty at the hearing.

According to the indictment, Zhang, 33, of San Jose, is alleged to have taken a confidential 25-page document containing detailed schematic drawings of a circuit board designed to be used in the critical infrastructure of a portion of an autonomous vehicle, knowing that the theft would injure the owner of the trade secrets, Apple, Inc.

Court documents filed in the case allege that on April 30, 2018, Zhang told Apple personnel that he was resigning from his job so that he could return to China to be closer to his mother who was ill. Apple immediately terminated Zhang's access to its computer systems and Apple personnel began a forensic analysis of Zhang's Apple-owned devices and network activity.

# Threats

- Example: Human action – deliberate - Malware
  - Malicious software deliberately designed to breach security of digital information systems
  - Depending on payload, malware can compromise
    - Confidentiality: For example, logging keystrokes to obtain passwords
    - Integrity: For example, by writing a message, or corrupting data files
    - Availability: For example, by deleting data or application files
  - Currently many cybercriminals using malware to take control of systems, and extort money from individuals or organisations to return access to systems and data – known as *ransomware*

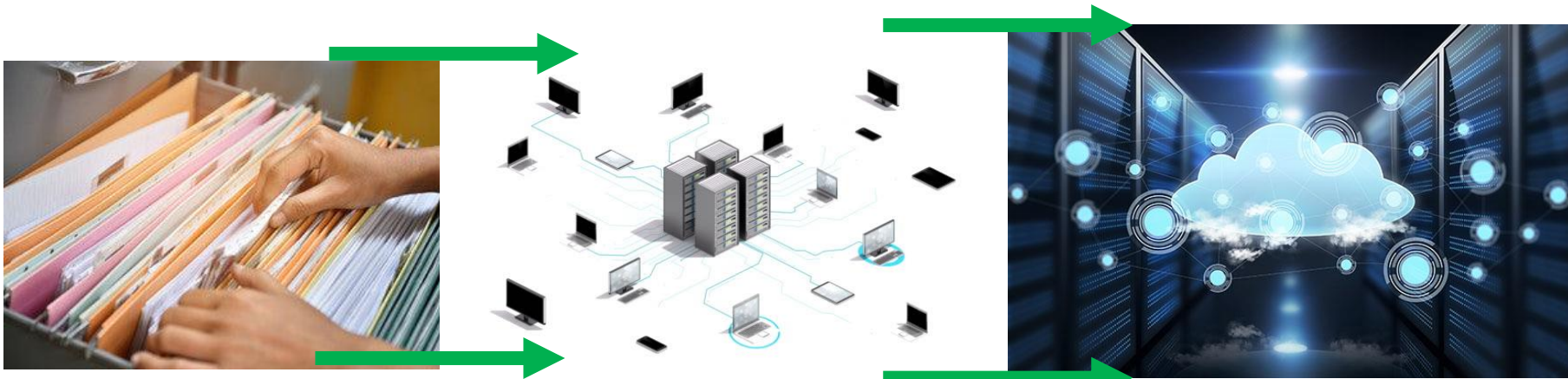
# Threats

- Human action – deliberate
  - *Common malware types*
    - Viruses – programs with ability to replicate
      - Spreads by copying itself into other files (infecting) and is activated when infected files are opened or exe's run
    - Worms – programs with ability to self-replicate
      - Spreads from computer to computer without human interaction
    - Trojan horses – programs with known desirable properties and hidden undesirable property
      - User downloads the program and knowingly uses desirable features
      - Undesirable feature runs without user knowledge



# Emerging technologies result in changes in the threat landscape

- means threat assessment must be ongoing



- Consider changes in document storage over time:

- **How** are documents stored?
- **Where** are the documents stored?
- **Who** can access the documents? What type of access?
  - Local/Remote?
  - Physical/electronic?

2025 – **What** can they do with/to the documents with potential for harm?

# Summary

- Many threats to information assets and systems
- To protect information assets, need to understand context:
  - What is the information asset?
  - Where is it located, and what state is the information in?
  - Possible threats – how could this asset be harmed?
- Why protect this information asset?
  - What is the value of the asset, and how critical is it?
  - Potential consequences if the asset is harmed?