

IFB240 Cyber Security

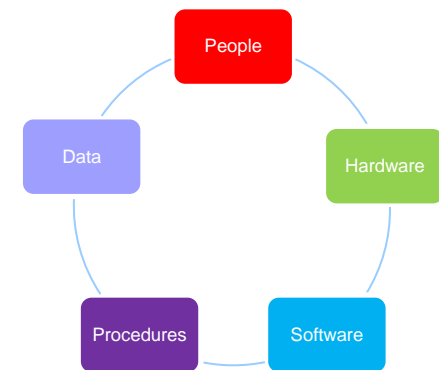
Lecture 2 - Part B Vulnerabilities

Dr Leonie Simpson

lr.simpson@qut.edu.au

Vulnerabilities

- Characteristics of, or weaknesses in, a system
 - that, if acted on by a threat, could cause harm to information assets
- Consider the components of information system
 - Property
 - People
 - Procedures
- Vulnerabilities exist in all of these



Vulnerabilities

- Property includes
 - **Physical assets:** buildings and contents
 - **Hardware:** computer systems, data communications devices, data storage devices
 - **Software:** Operating system, applications
 - **Data:** System and organisational data: files, databases, passwords, ...
- Consider possible vulnerabilities for each
 - This list is not exhaustive, just some of the possibilities...

Vulnerabilities

Property – physical assets

- Aspects to consider include
 - Location of information assets
 - In a geographical area that is:
 - Susceptible to natural disaster
 - Near storage of flammable or corrosive materials
 - Close to targets for disruption (may be collateral damage if neighbouring building is target)
embassy, military site
 - Easily accessed by outsiders?
 - Physical security mechanisms
 - Fences, walls, locks, gates, partitioning of internal space



Vulnerabilities

Property – physical assets

- Example: India, February 2024

fireworks factory explosion

[Eight Dead, 80 Injured in India Firework Factory Explosion \(voanews.com\)](https://www.voanews.com/news/india-firework-factory-explosion-20240206)

Eight Dead, 80 Injured in India Firework Factory Explosion



Rescue personnel and local residents gather near a firecracker plant following an explosion at Harda district in India's Madhya Pradesh state on Feb. 6, 2024.

NEW DELHI — At least eight people died and 80 were injured Tuesday in a giant explosion at a firework factory in India that saw balls of flames soar into the sky, officials said.

Related

[More Than 20 Dead After](#)

Vulnerabilities

Property – physical assets

- Aspects to consider include
 - Maintenance
 - Is asset in working condition?
 - Is perimeter protection maintained?
 - Monitoring and logging physical access
 - Use of suitable equipment for monitoring access to facilities and environmental conditions
 - Examples:
 - » CCTV, Intrusion Detection/Alarm system,
 - » Fire detection and automatic fire suppression system, etc
 - Do these depend on other systems – telecommunications, etc?

Vulnerabilities

- Property – ICT hardware and software
- Aspects to consider include
 - Reliability and robustness of
 - Asset
 - Susceptibility to environmental conditions (dust, heat, humidity)
 - Supporting infrastructure
 - Power supply, air conditioning, etc.
 - Redundancy
 - What happens if/when equipment fails?
 - Is there sufficient alternative resources?
 - Uninterruptible Power Supply (UPS),
 - What fail state does equipment revert to? (Open/closed?)

Vulnerabilities

- Property
 - ICT Hardware and software
- 2019/2020 Bushfires
- Mobile phone coverage dependent on power supply
- Powerlines destroyed in fires
- Significant loss of services

Telco, NBN failures during bushfire crisis reveals cracks in regional, rural crisis coverage

ABC Rural / By national regional and rural reporter Jess Davis

Posted 13 Jan 2020



Moruya residents were left without mobile and internet coverage on New Year's Eve as fire spread. (AP: Rick Rycroft)

Share



As fire rushed towards Moruya Heads on the NSW South Coast on New Year's Eve, Fiona Whitelaw and her family were relying on a wind change to save their house.

Unsure when it would arrive, they were continuously monitoring weather and fire information — but [then mobile coverage, the National Broadband Network \(NBN\) and the local ABC radio transmitter](#) all dropped out.

Key points:

- Residents whose communications were cut off during the bushfire crisis say infrastructure is not up to scratch

Vulnerabilities

Property – ICT Hardware and software

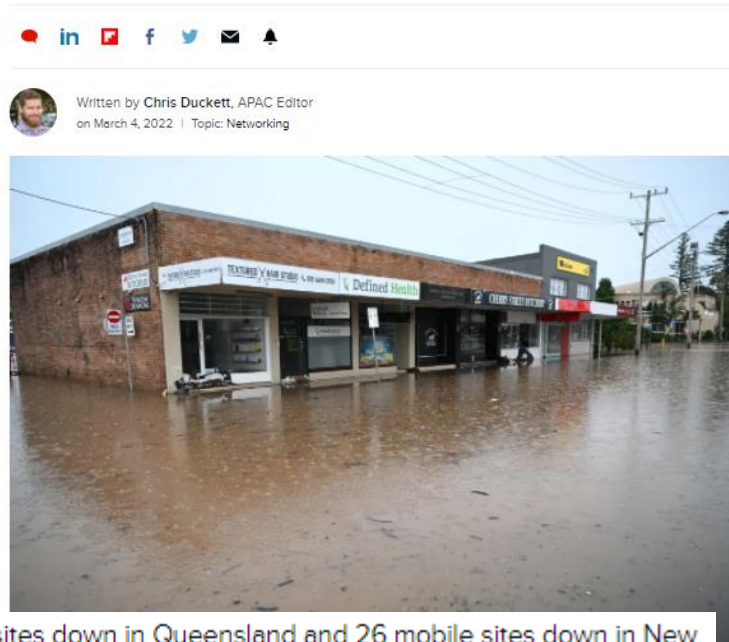
What is happening with telecommunications in flood-hit regions of Queensland and NSW

Site inaccessibility and lack of power means those in flood-affected areas are without connectivity even if they are dry.

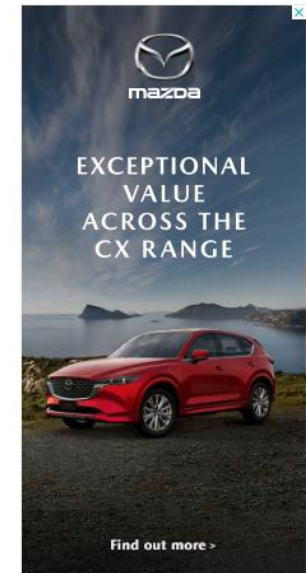
- **2022 Floods**

- Significant loss of services

- [What is happening with telecommunications in flood-hit regions of Queensland and NSW | ZDNet](#)



As of noon on Friday, Optus has 38 sites down in Queensland and 26 mobile sites down in New South Wales. The total number On Friday, the company responsible for the National Broadband Network said it has seen the total are individual sites. It does hav number of premises offline rise to 74,000 in northern NSW, while southeast Queensland was trending downward with 33,200 services offline.



Vulnerabilities

- Property – ICT hardware and software
- Aspects to consider include
 - Source of software: authorised, legitimate, vendor supported?
 - Still using Windows XP? Vendor support ended in 2014
 - Still using Windows 7? Vendor support ended Jan 2020
 - There will be no updates to correct vulnerabilities in software
 - Downloading and installing: what is permitted?
 - Can users install whatever software they like, obtained from wherever they like?
 - What processes are followed?
 - Could install software containing malware ☹

Vulnerabilities

- Property – ICT hardware and software
- Consider aspects including
 - Design, creation and testing of software
 - There are often flaws (bugs) in software
 - Example: common input problems: buffer overflows, injections
 - Possible that an attacker may exploit this
 - Need for patching and upgrading
 - Patch: Vendors make changes to software to correct bugs, and make the updated code available
 - Needs to be installed to be effective
 - How soon should the update be installed once it is available?
 - ACSC Annual Cyber Threat Report 2022 (p60) notes: ‘The time between vulnerability disclosure and exploit is closing rapidly; what once took weeks is now taking days or even hours.’
 - Are there other systems that may be impacted by an update? (dependency and compatibility issues)





Vulnerabilities



- Property – ICT hardware and software
- Consider aspects including
 - Configuration/misconfiguration
 - Has the system been implemented and set up appropriately?
 - Has the setting been changed from the default setting?
 - Is the default setting secure?

Misconfigured UTAS SharePoint site exposed 20,000 students' details

By Ry Crozier
Sep 21 2020
2:01 PM

0 Comments

RELATED ARTICLES

Cisco ships critical fix for IP phones

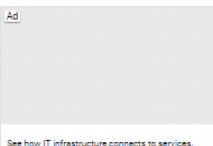

SA Water rewrites its tech strategy

Security settings allowed broad access to files.

A misconfigured SharePoint site led to the exposure of files containing the personal information of almost 20,000 University of Tasmania students to anyone with a university email address.

The University of Tasmania said in a statement that the incident came to light on August 11 but that it had only today contacted students.

It said the misconfiguration was active – and the files broadly accessible to anyone with a utas.gov.au email address – "from February 27 to August 11" of this year.



NETGEAR®

EXPLOITS AND VULNERABILITIES | NEWS

Update now! NetGear routers' default configuration allows remote attacks

Posted: December 8, 2022 by Pieter Arntz

NetGear has made a hotfix available for its Nighthawk routers after researchers found a network misconfiguration in the firmware allowed unrestricted communication with the internet facing ports of the device listening through IPv6.

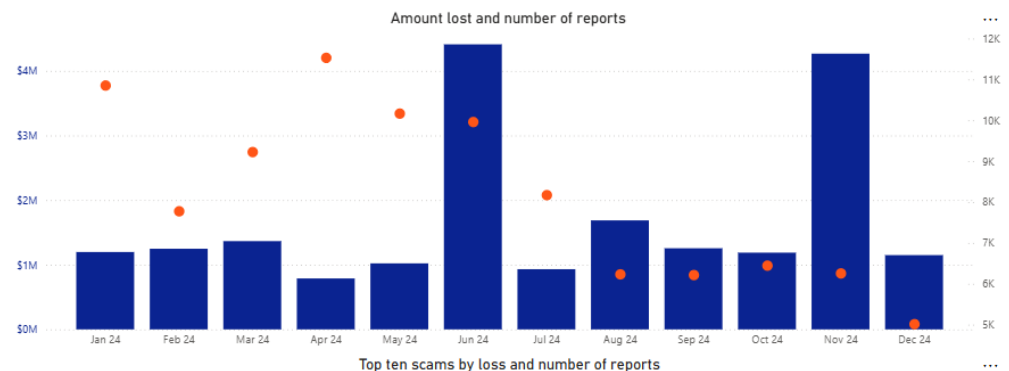
No auto-update

The hotfix is available for the model RAX30, also known as the Nighthawk AX5 5-Stream AX2400 WiFi 6

Vulnerabilities

People - Lack of awareness of threats

- Example - vulnerable to social engineering
 - ACSC defines social engineering as
 - ‘The methods used to manipulate people into carrying out specific actions, or divulging information.’
 - Lack of awareness that this occurs makes people vulnerable
 - ACCC Scamwatch figures:
 - 2024 Phishing statistics:
 - Amount lost: \$20, 510,354
 - Number of reports: 97,831



– Source:

– <https://www.scamwatch.gov.au/research-and-resources/scam-statistics>

Vulnerabilities

People – within organisations

- Example: Employees
 - Recruiting staff suitable for the position
 - Failure to check background is common
 - Monitoring access of people to property & processes
 - Disgruntled employees, clients or contractors can be exploited or threat source
 - Inadequate training and awareness of staff re threats
 - for example, are staff aware of policies regarding
 - providing information by email or over phone
 - downloading software
 - configuration of product
 - checking publicity photos before release, etc

Vulnerabilities

- Example: People – recruiting failure

THE AUSTRALIAN NATIONAL AFFAIRS BUSINESS AUSTRALIAN IT HIGHER EDUCATION VIDEO
Breaking News The Nation The World Features Opinion & Blogs Galleries Sport Health & Science E

New Zealand spy agency skipped basic procedures when hiring British fantasist

By staff writers | NewsCore | January 28, 2011 9:12PM A⁺ A⁻ Print Email S

 Recommend  15 people recommend this.  0 tweet  Share

NEW Zealand's spy agency failed to follow basic procedures when it granted security clearance to a top defence official who turned out to be a fantasist, Prime Minister John Key said today.

British-born Stephen Wilce was recruited in 2005 and appointed as chief defence scientist and director of New Zealand's Defence Technology Agency - after he provided a series of elaborate and extravagant lies about his past during the recruitment process, news website stuff.co.nz reported.

Wilce's false claims and vast exaggerations included that he served as a helicopter pilot with Britain's Prince Andrew, worked for British security services MI5 and MI6, played international rugby for Wales, was on a hit list for Irish terrorist group the IRA and competed against the Jamaican "Cool Runnings" bobsled team in the 1988 Winter Olympics.

Vulnerabilities

- Example: People – recruiting failure
 - Source: Brisbane Business News - January 2012

EMPLOYERS WARNED: RUN CHECKS OR RISK CRIMINALS

[< Previous](#)

[Next >](#)

By Jason Oxenbridge

Jan, 2012



QUEENSLAND companies are leaving themselves open to fraud risk by not performing criminal history checks on their prospective employees, according to a leading recruiter.

In light of the weekend's revelations of a Queensland Health employee allegedly defrauding the State Government of \$16 million, it has been revealed that only a fraction of employers conduct police background checks as part of the hiring process.

It is alleged Hohepa Morehu-Barlow had a history of fraud related offences in New Zealand, however his criminal background was not uncovered as checks were not performed.

Related News

RBA UNDER FIRE FOR NOT LOWERING INTEREST RATES

Volume 5, 06-02-2012

THIESS SECURES \$325M CSG CONTRACT

Volume 5, 06-02-2012

BATTERY WORLD CHARGED UP

Volume 5, 06-02-2012

LIGHTS OUT FOR SLEEP CITY

Volume 5, 06-02-2012

BRISBANE AGENCY CLEANS UP AT REAL ESTATE 'OSCARS'

Volume 5, 06-02-2012

Vulnerabilities

People – within organisations

- Example: People – lack of training and awareness – software download
- [A student pirating software led to a full-blown Ryuk ransomware attack \(bleepingcomputer.com\)](https://bleepingcomputer.com/news/a-student-pirating-software-led-to-a-full-blown-ryuk-ransomware-attack/)

A student pirating software led to a full-blown Ryuk ransomware attack

By [Lawrence Abrams](#)

May 6, 2021 12:08 PM 4



A student's attempt to pirate an expensive data visualization software led to a full-blown Ryuk ransomware attack at a European biomolecular research institute.

Vulnerabilities

People – within organisations

- Other aspects to consider include
 - Employees
 - Are there key personnel critical to organisation's operation?
 - May be unavailable due to accident or illness, or other event (transport failure, natural disaster, lotto win 😊)
 - May be uncooperative
 - Vulnerable if no back-up for these people
 - *Especially* if procedures they perform are undocumented
 - Others
 - Are security conditions included in contracts with consultants, contractors, outsourcing?

Vulnerabilities

Processes used

- Aspects to consider include
 - Access control and privilege management
 - What are the processes used for managing these?
 - Including keys, ID cards, passwords, ...
 - Backup of files and systems
 - Who does this?
 - When/How often?
 - Where are these stored? Encrypted storage or not?
 - Business continuity plans
 - For recovery of information assets after disaster
 - There is a plan, right?
 - Who knows about it? Has it been rehearsed? Is there a drill?

Vulnerabilities

Processes used

- Aspects to consider include
 - Communications
 - What is the acceptable use policy for communications systems
 - Example: confirmation for sending/receiving messages
 - » Will you know if a message has been misdelivered?
 - Does it matter *what* the message is?
 - Is it OK to email a new password to someone? Or should a different process be used?
 - Is it OK to login to a website using http and provide a PIN?
 - What about PIN for ATM card? Can that be sent in email?
 - Example: Passwords - see plaintextoffenders.com

Vulnerabilities

- Example: Communications processes
- How do you join a Zoom meeting?
Do you
 1. Go to Zoom, enter meeting ID and password? OR
 2. Click on the link in the Zoom invite?
- Why does this matter?
- Source: NZ Herald, 24 November 2020
- [Fake Zoom invite warning: The click that cost a hedge fund \\$8.7 million - NZ Herald](#)

Fake Zoom invite warning: The click that cost a hedge fund \$8.7 million

24 Nov, 2020 07:14 AM

5 minutes to read



Image / 123rf



By Chris Keall

Chris Keall is the technology editor and a senior business writer for the NZ Herald

[VIEW PROFILE](#)



Sydney hedge fund Levitas Capital has collapsed after one of its founders clicked on a link in a fake Zoom invite - which triggered a malicious software program to be planted on the company's network....

Vulnerabilities

Processes used

- Aspects to consider include
 - Checks and balances
 - People make mistakes: are there processes to detect, correct or reduce the impact of errors?
 - Example: Separation of duties
 - Processes associated with staff joining/leaving organisation
 - Clear statement of duties
 - Nondisclosure/confidentiality agreements
 - Software management processes and auditing
 - Application whitelisting?

Vulnerabilities

- Example: Is there a process to detect when people make mistakes?

- Source: <https://www.news.com.au/finance/work/at-work/a-major-financial-accident-samsung-employee-makes-140-billion-fat-finger-mistake/news-story/7c927c899c9a534ba8a82c63ccff34ba>

‘A major financial accident’: Samsung employee makes \$140 billion ‘fat finger’ mistake

A “FAT finger” mistake by a Samsung employee caused the company to accidentally hand over a whopping \$140 billion.



Frank Chung [@franks_chung](#)

news COMLAW APRIL 12, 2018 2:04PM


Video Image



A brief history of the mobile phone

SAMSUNG'S Korean stock trading arm is in turmoil after a \$140 billion “fat finger” mistake.

Last Friday, a Samsung Securities employee accidentally caused the company to pay out the massive dividend in the form of its own shares to more than 2000 employees who were members of the company stock-ownership scheme, *The Wall Street Journal* reported.




REAL PARTNERSHIP FOR REAL GROWTH.

Conditions apply

GET STARTED



VOSTRO 14 5000
Starting from \$1,499*



Intel Business Rewards

- Paying dividends
 - to employees owning shares
- Dividend payment error:
 - Instead of 1000 won per share issued dividend equal to
 - value of 1000 shares per share

Summary

- For information assets and their support systems
 - Many threats
 - Many vulnerabilities
- To protect information assets, need to understand
 - What the asset is, where it is, what the value is
 - Possible threats
 - Existing vulnerabilities
 - Likelihood of threats and vulnerabilities coinciding
 - Potential consequences if that does happen