

IFB240 Cyber Security

Lecture 2 - Part C

Security Incidents and Attacks

Dr Leonie Simpson

lr.simpson@qut.edu.au

Security Incidents and Attacks

- When threats and vulnerabilities coincide, information assets can be harmed
 - a security incident occurs
- Security incidents
 - Referred to as an attack if the threat involves deliberate human action
 - Attacker - Person who deliberately attempts to exploit a vulnerability to gain unauthorized access, or perform unauthorized actions (also called threat actor, malicious actor)
- NOTE: Even if threat action is not deliberate, damage from a security incident can still be extensive

Security incidents

- Example – August 2020 data breach Tasmania
- [Data breach at University of Tasmania affects 20,000 students - ABC News](#)

Data breach at University of Tasmania affects 20,000 students

By James Dunkley and Alexandra Humphries

Posted Mon 21 Sep 2020 at 1:58pm, updated Mon 21 Sep 2020 at 7:42pm



UTAS said there was "no evidence the breach was the result of malicious activity". (Supplied: UTAS)

The University of Tasmania has had to contact almost 20,000 students after their personal information was accidentally made accessible to all users with a UTAS email address.

The data that became accessible due to the breach varied for individual students but could have included birth dates as well as whether the student had a disability or identified as indigenous.

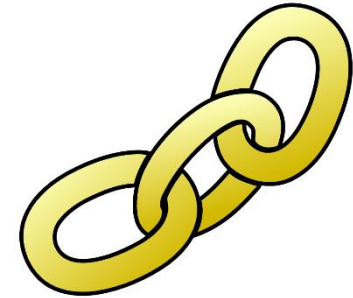
UTAS said there was "no evidence this data breach was the result of malicious activity" and that "security settings on shared files were unintentionally configured incorrectly, which made the information visible and accessible to unauthorised users".

accessed by individuals with a University of Tasmania email address".

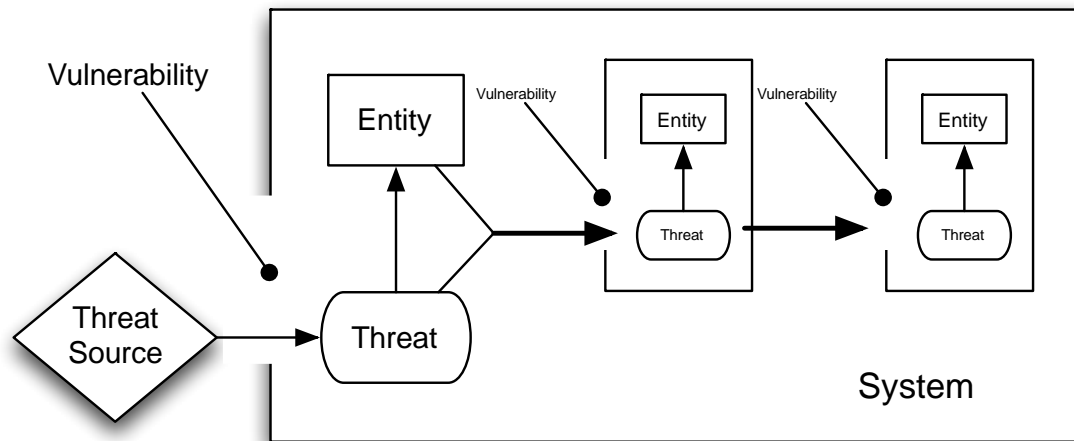
"The security settings for this SharePoint site were unintentionally configured incorrectly. This meant that individuals with a utas.edu.au email address not authorised to access documents saved in the site, were inadvertently granted access.

"This was the result of incorrect configuration. There is no evidence this data breach was a result of malicious activity. The system has now been correctly configured."

Chain of events in an incident



- When threats and vulnerabilities coincide, information assets can be harmed
 - Each event or incident can create new vulnerabilities
 - If these are exploited, subsequent security incidents occur
 - Sometimes there is a chain of events, especially in interconnected systems



Chain of events

- Example chain of events

- Event 1 – *Personal information exposed*

- **Vulnerability**: Misconfigured internet connected database containing personal information, including DOB, contact addresses, of students ...
- **Threat**: Personal information in database will be disclosed to unauthorised persons
- **Attack**: Unauthorised person deliberately accesses database, observes and copies personal information (breaches confidentiality)

- Event 2 – *Phishing the students*

- **Vulnerability**: Students susceptible to email phishing
- **Threat**: Email recipient opens attachment to email that contains malware, installs malware on their device
- **Attack**: An unsuspecting student receives a phishing email (body may be a friend request, birthday message, discount coupon attached, request to review attached invoice, etc), opens the attachment and the malware is installed on their device

Chain of events

- Example chain of events - continued
 - Event 3 – *Malware extracts information*
 - **Vulnerability**: Students computer allows them to install software, and/or their antivirus scanning software does not detect the malware in attachment or after installation
 - **Threat**: Key logging malware will be installed – information entered from keyboard will be recorded (say, passwords to other accounts, including online banking) and sent over network to attacker
 - **Attack**: Key logging malware used: after student victim has accessed accounts online, attacker now has record of phishing victim's credentials for other accounts (breaches confidentiality)
 - Event 4 – *Stealing money from student bank accounts*
 - **Vulnerability**: Student has online bank account that uses password as single authentication factor
 - **Threat**: Unauthorised person can access the bank account and perform transactions
 - **Attack**: Attacker uses victim's credentials (can provide correct credentials, so looks legitimate to bank system) to access victim's bank account and transfers money out of student's bank account (into a mule account – multiple used in path to attacker's account)

Types of attacks

- Categorised based on attacker interaction
 - Passive
 - Attacker's goal is to obtain information
 - Attacker **does not alter** information system resources
 - No interaction by the attacker other than listening or observing
 - Difficult to detect; usually try to prevent the attack
 - Active
 - Attacker's goal may be to obtain, modify, replicate or fabricate information
 - Requires some action or interaction with the information system by the attacker
 - Usual approach is to try to detect attacker's actions, recognise them as signs of attack and recover

Passive Attacks

- Eavesdropping

- Listening to conversations of others
 - Without their knowledge or consent
- Wiretapping
 - Eavesdropping over telephone network
 - May be harder to detect in wireless network
- Information can be obtained from
 - The content of the conversations, and
 - Knowing who is talking to who and when (traffic analysis)



Passive Attacks

- Shoulder surfing

- Watching the actions of others (especially at data entry) without their knowledge or consent
- Usually connected with entry of confidential information
 - PIN (for financial access at ATM)
 - Security code or password
- Can also be for greater amounts of data
 - Use of mobile devices in insecure surroundings is vulnerability that can be exploited for this attack



Passive Attacks

- Network monitoring and eavesdropping
 - A packet sniffer or network analyzer can monitor network traffic, can be used
 - For network maintenance (finding faults and traffic problems)
 - Or to gain knowledge of confidential information
 - For example, passwords corresponding to user names
 - Confidential information should not be sent over untrusted networks without protection
 - Example: when logging on to a remote resource, passwords should not be sent 'in the clear' (unencrypted)

Active Attacks

- Denial of Service (DoS) Attack
 - Objective is to make an information asset or resource unavailable to authorized users
 - Common methods used by attackers are
 - Damage the resource, so that it cannot be used
 - Deliberately interrupt communications between users and resource, so that it cannot be accessed
 - Overload the resource by making a large number of requests for service, so it cannot respond to legitimate requests
 - Vulnerability - exists in information system providing service
 - Threat - that the service will be made unavailable
 - Attacker - deliberately exploits vulnerability to achieve this

Active Attacks - Examples

- Example: Denial of Service (DoS) Attack
- Can also apply to telecommunications (TDoS)
 - Mirai malware in Nov 2016 attack on Deutsche Telekom
 - <https://www.itnews.com.au/news/mirai-botnet-attacks-900000-german-broadband-routers-442887>

Mirai botnet attacks 900,000 German broadband routers



Malware attempts to infect routers via remote management feature.

Hundreds of thousands of Deutsche Telekom broadband customers in Germany have been attacked by the Mirai malware, crashing their routers and degrading internet connections.

The telco **said** as many as 900,000, or about 4.5 percent of its 20 million fixed-line customers, began to have problems connecting to its network on Sunday afternoon.



Active Attacks

- Distributed Denial of Service (DDoS) Attack
 - Objective is same as DoS attack
 - Breaches availability of information asset
 - *Slight difference* in method
 - Use *multiple* sources to make resource requests
 - Malware (virus) may be used to first compromise machines and make them bots in a net controlled by an attacker → botnet
 - All bots have same target and payload is activated at same time, to make simultaneous resource request
 - Overloads resource, so it cannot respond to legitimate requests

Active Attacks - Examples

- Example: Denial of Service (DoS) Attack
 - DoS and DDoS commonly applied to websites
- Feb 17 2023 The Record
 - [German airports hit by DDoS attack, 'Anonymous Russia' claims responsibility - The Record from Recorded Future News](#)



IMAGE: ALAN ANGELATS VIA UNSPLASH

Daryna Antoniuk
February 17, 2023

Briefs



German airports hit by DDoS attack, 'Anonymous Russia' claims responsibility

It's been a difficult week for German airlines.

A day after a major IT failure at Lufthansa left thousands of passengers stranded, the websites of seven airports were hit by a suspected cyberattack.

Among the airports affected by a "large-scale DDoS [distributed denial-of-service] attack" on Thursday were Dusseldorf, Nuremberg, Erfurt-Weimar and Dortmund, according to Ralph Beisel, chief executive of the ADV airport association.

The airports' websites were temporarily down, but are up and running again as of Friday. The websites of Germany's biggest airports in Frankfurt, Munich and Berlin were not targeted.

Active Attacks

- Masquerade/Spoofing
 - One entity pretends to be another to deceive others
 - Exploits human vulnerability
- Common spoofing attacks include
 - Caller ID spoofing
 - For phone calls, showing false caller ID or number
 - Email address spoofing
 - Altering the sender information on email to trick recipients into thinking the message is from another source
 - Webpage spoofing
 - Creating a fake webpage that looks like the page for a legitimate business to trick users
 - into giving up credentials they use at legitimate site
 - into downloading materials from an alternative site

Active Attacks

- **Social Engineering**
 - Using social skills to convince people to reveal information or permit access to resources
 - Can happen in person, or by email, phone, text, ...
 - **Examples**
 - **Claim to be new employee**, manager's assistant, maintenance person, etc
 - Ask for assistance in accessing resource to complete an urgent task
 - I've lost my password and I have to finish this today ...
 - My swipe card doesn't work/left at home ...
 - **Tailgating** – follow another person closely, so that when they go into secure area you can also get in without providing appropriate credentials

Active Attacks

- Phishing

- Usually involves

- Spoofing (sender email address or caller ID, and/or web pages) + social engineering

- Method used

- Attacker initiates communication aimed at gaining information
 - Especially credentials to gain access to other resources
 - Example: account details, PIN number, password
 - Masquerades as a legitimate organisation you may have a relationship with (Bank, eBay, PayPal, Tax Office, Police, ...)
 - Motivates user to respond urgently
 - With threat of penalty (Your account will be locked ...)
 - Or promises of reward (First X replies gain a \$\$\$ credit ...)

Active Attacks

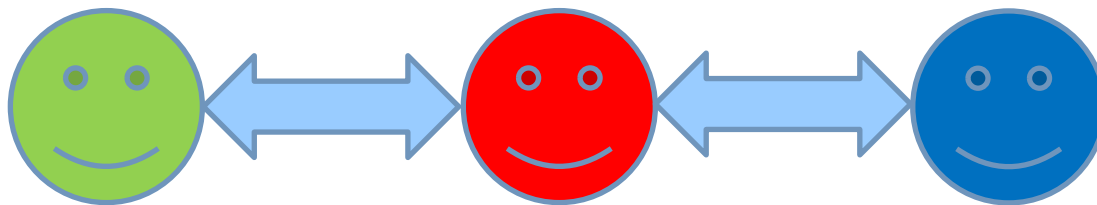
- Man-in-the-Middle Attack (MITM)

- [Machine-in-the-Middle Attack (MITM)]

- An attacker (Carol) positions themselves between two entities who wish to communicate, say Alice and Bob.

- Carol

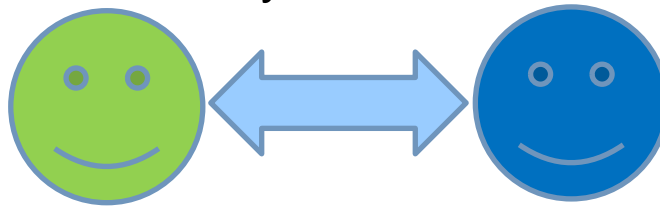
- pretends to Alice she is Bob and
 - pretends to Bob she is Alice (spoofing both ways)



Active Attacks

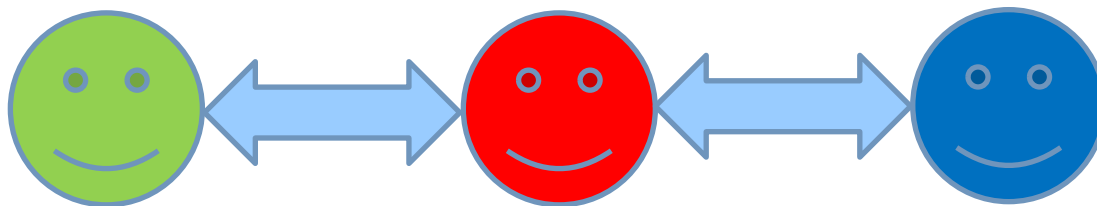
- MITM

- Alice and Bob think they are communicating with each other:



- **However** all messages between them go via Carol, so Carol can control the conversation

- Could just monitor conversation (breaches confidentiality)
 - Can also insert or modify information (breach integrity)
 - Could even delete messages, prevent delivery (breach availability)



Active Attacks

- MITM
 - Vulnerability: no authentication of the communicating endpoints
 - That is, you assume that the entity you are communicating with is who they say they are
 - But you do not have any check in place to be sure they are
 - A threat actor can exploit this vulnerability

Active Attacks

- Replay attack
 - A valid data transmission is captured (recorded), stored and retransmitted at a later time
 - Example
 - Access to a system requires use of password, but password is encrypted during transmission
 - Attacker records encrypted password, and replays this information at another time to gain access
 - Doesn't matter that attacker doesn't know the password – they can provide the expected credential on request

Case study: Ransomware

- Threat

- Access to information system (phone/computer/network) will be restricted OR
- Confidential data will be published (OR BOTH)
 - Restriction lifted upon payment of ransom
 - Examples: Cryptolocker, Locky, WannaCry – files encrypted
 - Pay fees to attacker to obtain the decryption key

- Vulnerability

- People (if introduced by phishing email), processes

- Attack

- Active or passive? Consider interactions and intent

- Control measures?

Case study: Ransomware

- [REvil ransomware to blame for UnitingCare Queensland's April attack | ZDNet](#)
- May 2021
- Affected UnitingCare systems
 - Hospitals
 - Aged care centres
- Threat actor: Revil
 - Ransomware Evil
 - Ransomware-as-a-Service
- Cybercriminals – interested in obtaining ransom payment \$\$\$
- Allegedly targeted other organisations
 - May 2021 - JBS Meat processing company

REvil ransomware to blame for UnitingCare Queensland's April attack

The healthcare organisation has confirmed the cyber incident it experienced last month was the result of a hit from REvil ransomware.

By Asha Barbaschov | May 5, 2021 – 22:54 GMT (08:54 AEST) | Topic: Security



Image: Getty Images

After revealing late last month it had fallen victim to a cyber incident, UnitingCare Queensland has now named REvil/Sodin as the gang behind the attack.

The organisation, which provides aged care, disability supports, health care, and crisis response services throughout the state, suffered the attack on Sunday, 25 April 2021.

In a statement issued a few days later, UnitingCare said its systems were still hurting. On Wednesday, it said some of the organisation's systems have since been inaccessible.

The organisation also pointed the blame at REvil/Sodin as the source of the attack.

"We can confirm that the external group claiming responsibility for this incident has identified themselves as REvil/Sodin," it said.

MORE FROM ASHA BARBASCHOW



Innovation
SMT partners with Intel and AARNet for new AWS cloud supercomputing facility



Security
ANAO: Auditing not driving improvements in Commonwealth cybersecurity adherence



Finance
Australia's largest bank accuses Apple of leaning on its market power



Innovation
Australia hears case for open access to Apple NFC tech as QR codes will not do

NEWSLETTERS

ZDNet Security

Your weekly update on security around the globe.

Summary

- For information assets and their support systems
 - Many threats and many existing vulnerabilities
- If threats & vulnerabilities coincide security incidents occur
 - Result in breaches of C, I, A
 - Called **attacks** if deliberate human action is involved
 - Lots of different types, lots of different targets
 - Severity of impact depends on
 - Value and criticality of asset
 - Degree of compromise
 - Perspective
- Incidents may happen in isolation, or may be part of a chain of events
- Consequences can be devastating for orgs & individuals

IFB240 Cyber Security

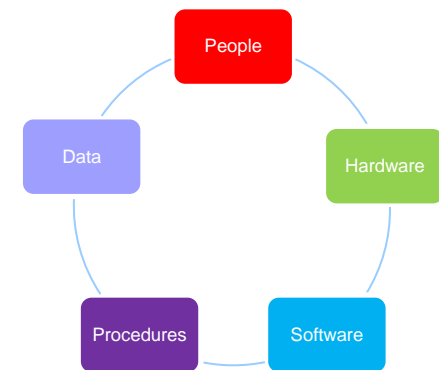
Lecture 2 - Part B Vulnerabilities

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

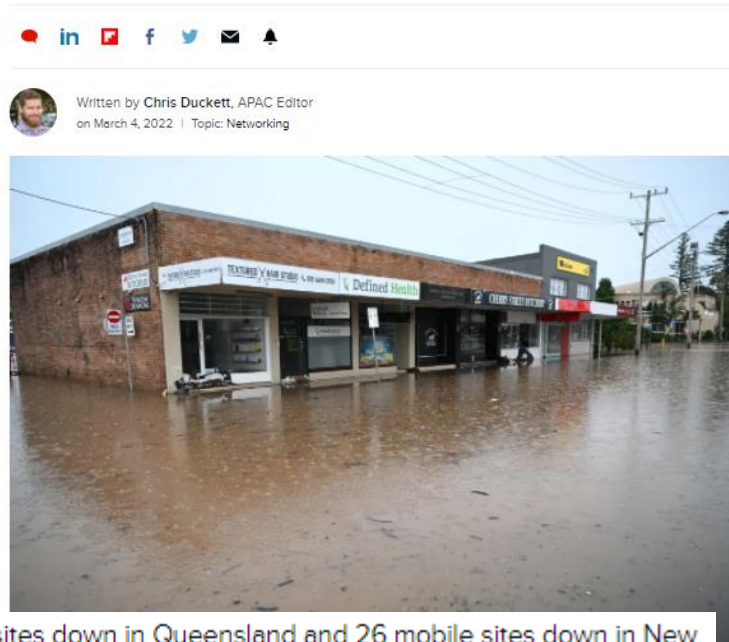
What is happening with telecommunications in flood-hit regions of Queensland and NSW

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

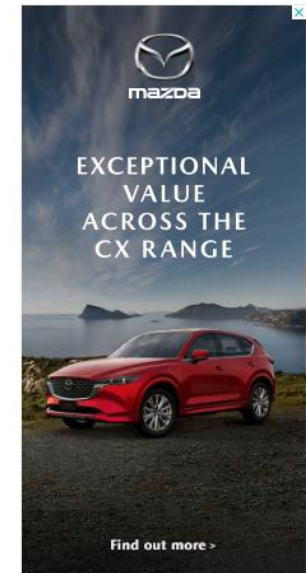
- **2022 Floods**

- 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.



RELATED

< . . . >

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

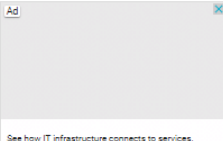

SA Water rewrites its tech strategy

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.

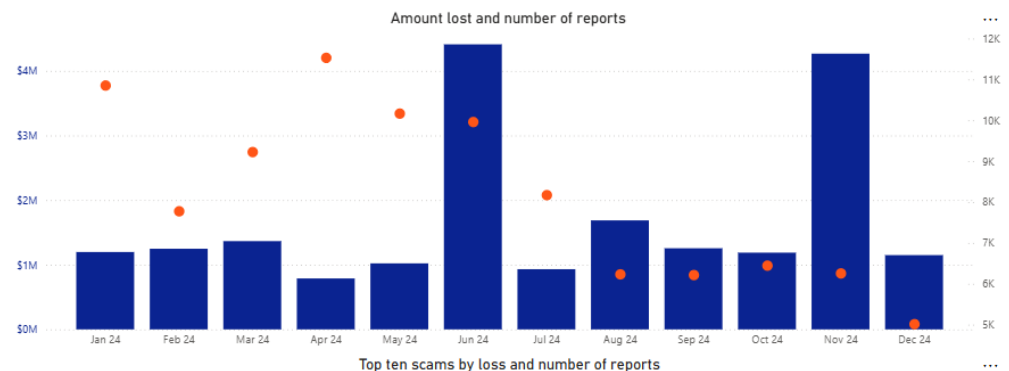
No auto-update

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 **COMET** 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.

DELL SMALL BUSINESS

REAL PARTNERSHIP FOR REAL GROWTH.

Conditions apply

GET STARTED

VOSTRO 14 5000
Starting from \$1,499*

Product of BUSINESS REWARDS

Intel vPro

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