

# INB255 Security

## Lecture 1: Introduction to Security


# Should you be here?

- Incompatible units:
  - You should not take this unit if you have successfully completed the unit:
    - ‘Data Security’ or ‘Information Security ...’ in previous semesters
    - Unit codes include: ITB/N161, ITZ161, ITN511, ITB/N523, ITZ523, ITB543, ITN582, ITB623, ITN663, ITB730, ITN730
    - INB255 Security (for potential INN255 students)
- Prerequisite units: none.
- Co-requisite units: none.

# Outline

- Acknowledgement of Traditional Owners
- Housekeeping:
  - Safety Awareness
  - Code of conduct for lectures
- Introduction to the Unit:
  - Staff
  - Structure
  - Content
  - Assessment
  - Resources
- Why study Security?
- Introduction to Information Security



The background of the slide is a traditional Indigenous Australian artwork. It features a dark, textured ground with intricate, flowing lines in shades of brown and ochre. These lines form stylized, swirling patterns that resemble smoke or water. Interspersed among these lines are numerous small, yellow and white dots, some arranged in straight lines and others in more scattered patterns. The overall effect is one of dynamic movement and cultural depth.

# Acknowledgement of Traditional Owners





# Acknowledgement *of* Traditional Owners

In keeping with the spirit of Reconciliation,  
I acknowledge the Turrbal, Jagera/Yuggera, Kabi Kabi and  
Jinibara Peoples as the Traditional Owners of the lands  
where QUT now stands – and recognise that these have  
always been places of teaching and learning.

I wish to pay respect to their Elders – past, present and  
emerging – and acknowledge the important role Aboriginal  
and Torres Strait Islander people continue to play within  
the QUT community.

**[www.reconciliation.qut.edu.au](http://www.reconciliation.qut.edu.au)**

# Outline

- Acknowledgement of Traditional Owners
- Housekeeping:
  - Safety Awareness
  - Code of conduct for lectures
- Introduction to the Unit:
  - Staff
  - Structure
  - Content
  - Assessment
  - Resources
- Why study Security?
- Introduction to Information Security

# Safety Awareness

- Evacuation route from this room:
- Assembly location:
- Returning to the room:

# QUT Student Code of Conduct

- From Chapter E/2.1 of QUT MOPP:
  - “ ... students are expected to:
    - treat other members of the University community with respect and courtesy
    - behave in a manner which does not adversely affect the freedom of other members of the University community to pursue their studies, duties or activities”
  - For our classes, please:
    - turn off your phone, or set to silent
    - if you use your laptop, keep it to 255 class activities to aid your learning and avoid distracting others
    - if you are late arriving, come in quietly and take a seat



# Outline

- Acknowledgement of Traditional Owners
- Housekeeping:
  - Safety Awareness
  - Code of conduct for lectures
- Introduction to the Unit:
  - Staff
  - Structure
  - Content
  - Assessment
  - Resources
- Why study Security?
- Introduction to Information Security

# Staff

- Unit Coordinator and Lecturer:
  - Dr Leonie Simpson
- Other Lecturers:
  - Dr Ernest Foo, Mr Malcolm Corney
- Other unit staff:
  - Tutors: Nischal Kush, Ben Dowling, Raphael Amoah
- Our contact details (email, phone, room location, etc) are on the 255 Security Blackboard sites (under **Contact Us**)

# Staff: Who do I contact?

- **Lecturer or Tutor**
  - for help with unit materials
    - For example: lecture material or workshop questions
- **Unit co-ordinator**
  - for most unit related matters
    - For example: attendance problems, exam marking
- **Administration – Student Services**
  - for some matters external to this unit
    - For example: enrolment problems, assessment extension requests, tutorial allocation issues
- **Disability Services**
  - for assistance to meet specific needs

# Contact details for Administration & Disability Services

- Administration:

- Student Services Counter, Level 3, O Podium, Gardens Point
- Email: [sef.enquiry@qut.edu.au](mailto:sef.enquiry@qut.edu.au)
- Phone: (07) 3138 2782

- Disability Services:

- A disability includes any impairment or medical condition, which may affect a student's ability to undertake a program of study successfully.
- A disability may be permanent, short-term or episodic in nature
- Details of support services available see:
  - <http://www.disabilityservices.qut.edu.au/>
- Make an appointment to discuss options as soon as possible

# Structure

- When do I have to attend?
  - Lectures: One 2-hour lecture per week
    - Lecture outlines made available on Blackboard site prior to the lectures
    - Download these, or print as handouts and bring to lectures as a note-taking aid
  - Tutorials: 1-hour tutorial session per week
    - Set questions are available on the Blackboard site
    - Prepare your written solutions prior to attending and bring them with you (allow 5-6 hrs/week for preparation and study).
    - Be prepared to participate in discussion, and take notes on points raised/make corrections to your solutions or notes.



# Why come to lectures/tutorials?

- QUT: MOPP E/2.1.3
  - “ ... students are expected to work to the best of their abilities and to make genuine attempts to progress successfully by meeting ... deadlines for assessment and by regular attendance and/or engagement with learning activities”
- Get better results:
  - From previous semesters, high correlation between
    - students with Security grade < 4 and poor class (lecture and tutorial) attendance
    - students with Security grade = 7 and excellent class (lecture and tutorial) participation
- Some advice from previous students:
  - If you can't commit to the few hours required for the lecture/tutorial, when will you find the time to study the materials?
  - It's easier to clarify points you don't understand in the lecture/tutorial time than by emailing tutors later
  - University subjects aren't cheap – so make the most of the available resources

# INB255 Unit Content

- See the Blackboard site for schedule, abbreviated form is:

Week	Topic	Assessment task
1	L1: Introduction to Security	Workbook
2	L2: Threats, vulnerabilities and attacks	Workbook
3	L3: Privacy and Security	Workbook
4	L4: Managing Security	Workbook
5	L5: Access Control Principles	Workbook
6	<i>No regular lecture – QUIZ in class time</i>	Workbook & In-class Quiz 1
7	L6: Symmetric Cryptography	Workbook & Security News Log 1
8	L7: Asymmetric Cryptography and PKI	Workbook
		Workbook
9	L8: Access Control Mechanisms	Workbook
10	L9: Digital Forensics	Workbook
11	L10: Network Security	Workbook
12	<i>No regular lecture - QUIZ in class time</i>	Workbook & In-class Quiz 2
13	L11: Review Lecture	Workbook & News Log 2
Exam block	Centrally timetabled written exam	Final Exam

# Content

## What is this unit about?

- This unit is about information security
- You will need to:
  - understand fundamental information security concepts
  - apply those concepts to situations:
    - both familiar and unfamiliar
  - think about the implications of certain actions or events
  - understand the limitations of certain actions
- It is **not**:
  - just about memorizing a heap of facts
  - a “how to hack a website/database/network” course
  - a training course to get a physical security job
    - For example, nightclub bouncer



# Assessment – INB255

- Assessment item 1 (40% of final grade)
  - Workbook/Log
    - 20% for record of your solutions to selected tutorial questions
    - 20% for Security News Log – submission via Assignment Minder
- Assessment item 2 (20% of final grade)
  - Quiz during lecture timeslot
    - a) Quiz 1 covers first 5 lectures
    - b) Quiz 2 covers last 5 lectures
  - Mark used for calculating result is your best of these 2 marks
- Assessment item 3 (40% of final grade)
  - Final examination – held during exam block

# Resources

- **Blackboard Website:**
  - <http://blackboard.qut.edu.au> (or Blackboard link from QUT homepage) then enter the unit code INB255 or select link
    - CUO, staff contact details, lecture outlines, workshop questions, assessment items etc.
- **Recommended Text:**
  - No set text, but there are lots of useful information sources available:
    - **In the library** - most introductory Information Security or Computer Security texts
    - **Online** – lots of useful Information Security sites (see workshop questions)
- **Standards Documents:**
  - Access [SAI Global – Standards Online](#) through QUT library:
  - Look for Databases, then go to Standards, and you will find the link for this one.
    - Lots of Australian Standards documents related to Information Security available.



# Unit feedback from last year

- INB255/INN255:
  - Best aspects of the unit:
    - The tutorial content and questions good for keeping up to date
    - Feedback on assessment extremely helpful
    - The two half-semester quizzes – an opportunity to improve, and makes you learn before the final exam
  - Aspects to improve on:
    - The standards documents are pretty boring (but useful, professionally)
    - More explanation of crypto, keys and hashing
- The teaching team for the Security unit appreciates your feedback 😊

# Outline

- Acknowledgement of Traditional Owners
- Housekeeping:
  - Safety Awareness
  - Code of conduct for lectures
- Introduction to the Unit:
  - Staff
  - Structure
  - Content
  - Assessment
  - Resources
- Why study Information Security?
- Introduction to Information Security

# Why study information security?

- Consider these items of personal information:
  - Name
  - Date of birth
  - Address
  - Financial details
  - Medical/Health details
  - Relationships (family/friends)
  - Membership details (clubs, societies, religious affiliation)
  - Details of your
    - Phone conversations
    - Shopping
    - Browsing
- Which of these would you be comfortable for others to access?

# Why study information security?

- Which of these would you be comfortable for others to access?
  - Name, Date of birth, Address
  - Financial details and/or Medical/Health details
  - Relationships (family/friends)
  - Membership details (clubs, societies, religious affiliation)
  - Details of your
    - Phone conversations
    - Shopping
    - Browsing
- Does your answer depend on:
  - The type of access? (Read only, read/write, ...)
  - The type of information?
  - Who the 'others' are?

# Why study information security?

- Consider these items of corporate information:
  - Names and addresses of
    - employees,
    - customers,
    - suppliers
  - Financial details of employees, customers, suppliers
  - Transaction records
  - Documents related to
    - Tenders for upcoming contracts
    - Details of upcoming promotions/campaigns
    - System configuration and management processes
  - Product development information
  - Trade secrets (secret recipe/formula/special process)
- Which of these would the organisation be comfortable for others to access?



# Why study information security?

- Which of these would the organisation be comfortable for others to access?
  - Names and addresses of employees, customers, suppliers
  - Financial details of employees, customers, suppliers
  - Transaction records
  - Documents related to
    - Tenders/promotions/campaigns/research findings
    - System configuration and management processes
  - Product development information
  - Trade secrets (secret recipe/formula/special process)
- Does your answer depend on:
  - The type of access?
  - The type of information?
  - Who the 'others' are?

# Why study information security?

- Consider some information items related to critical infrastructure:
  - Locations and functions of essential facilities for various industry sectors:
    - Agriculture and biosecurity
    - Defence
    - Energy
    - Finance
    - Transport (planes, trains, automobiles ...)
    - Telecommunications
    - Water and waste management and distribution
  - Details of the control systems for these networks:
    - Documents related to configuration and management processes
    - Details of protective measures (or lack of)
- Which of these would a nation be comfortable for others to access?

# Why study information security?

- Which of these would a nation be comfortable for others to access?
  - Locations and functions of essential facilities for various industry sectors:
    - Agriculture and biosecurity, Defence, Energy, Finance
    - Transport (planes, trains, automobiles ...), Telecommunications
    - Water and waste management and distribution
  - Details of the control systems for these networks:
    - Documents related to configuration and management processes
    - Details of protective measures (or lack of)
- Does your answer depend on:
  - The type of access?
  - The type of information?
  - Who the 'others' are?

# Outline

- Acknowledgement of Traditional Owners
- Housekeeping:
  - Safety Awareness
  - Code of conduct for lectures
- Introduction to the Unit:
  - Staff
  - Structure
  - Content
  - Assessment
  - Resources
- Why study Security?
- Introduction to Information Security

# What is Security?

- Security is about the protection of assets from damage or harm.
- Assets are items or processes that are of value
  - Can include:
    - Property
      - For example: buildings, ICT hardware, storage facilities
    - People
      - Who is of value, at various levels?
        - » Personal, Corporate/Organisation, National
    - Intangibles
      - Image, Reputation



# What is Security?

- Some examples:
  - Personal assets:
    - Property: Your house, car, laptop, phone, jewellery
    - Intangible: Your online reputation, your credit rating
  - Organisational assets:
    - Property: Buildings, servers, laptops, products, IP
    - People: CEO, Service manager, PA, scientist
  - National Assets:
    - Property: Buildings, Agricultural lands, Infrastructure
    - People: Government employees, Development staff

# What is Security?

- For effective protection you need to know:
  - What your assets are
    - Example: home contents
  - What they are worth, and how critical they are
    - Could you replace them? How hard is it to live without them?
  - What could possibly happen to affect them
    - Consider accidental and intentional events
  - How they could be protected, and at what cost?
    - Consider possibilities for:
      - Prevention of damage to asset (or minimising damage)
      - Detection of damage to asset – when, how, who?
      - Reaction to recover from damage

# What is Information Security?

- Information is an important asset:
  - What sort of information is important/essential?
    - For you, as an individual
    - For organisations
    - For Australia, as a nation
  - For particular assets, how valuable are they (what is the cost if it is lost or damaged)?
    - Financial loss
    - Impaired performance
    - Loss of competitive advantage
    - Loss of reputation
    - Violation of legislation (penalty may apply)

# What is Information Security?

- **Information Security** is about protecting information assets from damage or harm
- Same questions to address:
  - What are the assets to be protected?
    - And how valuable are they?
  - What could possibly happen to them?
    - Consider accidental and intentional events
  - How can I protect my assets?
    - Consider
      - Prevention: of damage to asset
      - Detection of damage to asset – when, how, who?
      - Reaction – to recover from damage
  - What does this protection cost? Is it worth it?

# Information Security

- Is there really a problem?
  - Lots of news stories about internet threats:
    - Cyber-crime
    - Hackers
    - Software flaws
    - Viruses
    - Denial of service (DoS) attacks
    - Privacy breaches
  - How many people does this impact?
  - <http://www.internetworldstats.com/stats.htm> (Current = June 30, 2012)

Region	Population	Internet users 2000	Current Internet users	% of Pop'n	Growth
Oceania/ Australia	35,903,569	7,620,480	<b>24,287,919</b>	67.6 %	218.7 %
World	<b>7,017,846,922</b>	360,985,492	<b>2,405,518,376</b>	<b>34.3 %</b>	<b>566.4 %</b>

# Information Security

- Is there really a problem?
  - **Cyber-crime** usually refers to electronic crime where:
    - Information and communications technology is the target
      - Examples: Intrusions (Hacking), Computer viruses, Denial of Service

Or

- technologies are used as tools to enable the offence
  - Examples: Phishing, Identity theft, Spam
- Growth in Internet usage makes this increasingly likely
  - Traditional crimes: theft, fraud, vandalism, etc using new technology

# Information Security

- Is there really a problem?
  - In 2007, McAfee Virtual Criminology Report 2007 noted three major trends in cyber-crime:
    - Increasingly sophisticated web espionage threat to national security
    - Growth in attack techniques threaten online services
    - A developing market in software flaws that can be used to carry out espionage or attacks
  - What has changed in the 7 years since then?

# Information Security

- The current state of cyber-security:
  - 2013 (2012) Cost of Cybercrime study (US) found
    - Avg annual cost per organisation: \$11.6 million (8.9)
    - Avg number of successful attacks per organisation: 122 (102)
    - Compared to 2012 figures,
      - Number of cyberattacks increased by 18%
      - Cost of cyberattacks increased by 26%
    - Most costly cybercrimes per organization result from:
      - denial of service, malicious insiders and web-based attacks
      - (malicious code, denial of service, stolen or hijacked devices, and malevolent insiders).
- [http://media.scmagazine.com/documents/54/2013\\_us\\_ccc\\_report\\_final\\_6-1\\_13455.pdf](http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf)
- <http://www.informationweek.com/security/attacks/cybercrime-attacks-costs-escalating/240008658>



# Information Security example:

- **April 2011: Sony PlayStation Network Outage**
  - April 17-19: malicious external attacker accessed Sony network
  - April 20: Sony suspended all PSN online services, worldwide
  - May 2: Sony issued press release – Sony Online Entertainment services offline due to maintenance related to PSN breach – expected return to service within a week
  - May 4: Sony confirmed personally identifiable information may have been stolen from each of the 77 million accounts
    - customer names, birth dates, addresses, email accounts, passwords, etc
  - May 15: Sony began to restore PSN services in North America
  - May 16: began to restore services in Australia
- Sony estimated costs of outage at US\$171 million

# Information Security example:

- March 2011 RSA security firm breached
  - Major product is SecureID tokens used by workers to log on to company networks



RSA SecurID SID700

- RSA reported breach but did not reveal which assets were compromised
- May 2011 security breach at US defense contractor Lockheed Martin
  - Said data for RSA Secure ID tokens used to aid network intrusion
  - Lockheed Martin replaced 45,000 Secure ID tokens used by their employees

# Information Security example:

- 2012 Global Payment Systems Data breach:
  - US company providing credit and debit processing and payment services for Visa and Mastercard
    - Directs payments between merchants and banks
  - March 2012 identified unauthorized access into processing systems
    - Breach occurred between January 21 and February 25
    - Admitted card data could be exposed
    - Estimates that around 1.5 million accounts compromised
  - Consequence:
    - Visa removed GPS from it's list of approved service providers until it demonstrates compliance with standards
- <http://www.zdnet.com/blog/btl/global-payments-data-breach-is-contained/72895>

# Information Security example:

- 2012 LinkedIn breach:
  - June 2012 LinkedIn confirmed passwords of over 6 million accounts compromised
- <http://www.reuters.com/article/2012/06/06/net-us-linkedin-breach-idUSBRE85511820120606>
  - File containing 6.4 million unsalted password hashes posted to Russian hacker forum
  - Attacker can use offline attack to recover passwords, then use passwords to access user accounts
- NOTE: Many similar previous breaches
  - E.g. RockYou breach in 2009 - over 30 million email addresses and plaintext passwords (not hashed) were accessed
  - Penalty applied by US FTC includes US\$250,000 payment and submission to security audits for next 20 years

# Information Security example:

- 2014 Australian Government breach:

## Immigration Department data lapse reveals asylum seekers' personal details

Exclusive: online database provides personal details of almost 10,000 people in serious and embarrassing security breach

[Oliver Laughland](#), [Paul Farrell](#) and [Asher Wolf](#)



[The Guardian](#), Wednesday 19 February 2014 13:57  
AEST [Jump to comments \(492\)](#)



Asylum seekers' identities became accessible online. Photograph: Colin Murty/Newspix/REX

The personal details of a third of all asylum seekers held in Australia – almost 10,000 adults and children – have been inadvertently released by the Department of Immigration and Border Protection in one of the most serious privacy breaches in Australia's history.

# Information Security example:

- Cyber crime enabled by technology - Phishing attacks
  - Begin with a spam email claiming to be from a legitimate organisation, and requesting personal information
  - A link in the email may direct users to a bogus site

## Important Notice: 3rd attempt failed !

To help protect your privacy, some content in this message has been blocked. If you are sure that this message is from a trusted sender and you want to re-enable the blocked features, [click here](#).

ANZ Bank [iwlrq@anz.com.au]

**Sent:** Thursday, 14 February 2013 1:33 PM

**To:** ips@iawcouncil.asn.au; ipsocijc@aol.com; Leonie Simpson; irescaia@inug.com.au;  
lriboldi@royfree.org.au; lrstone@austarnet.com.au; lrungie@unimelb.edu.au;  
lrussell@saron.com.au; ls.canning@bigpond.com; lsansom@nexus.edu.au;  
lsc@larasportingclub.com.au; lsenese@westpac.com.au; lsi@garion.it.com.au;  
lsmith@mercedes.wa.edu.au; lsn@business.auc.dk; lso@dhm.com.au;

Dear ANZ Bank Customer,

Within ANZ Bank latest security checks, we recently discovered that today there were 3 incorrect login attempts to your account.

For your safety, ANZ Bank set your account status to limited. **For your account status to get back to normal, you will have**

**to Sign In correctly at:** <https://www.anz.com/INETBANK/bankmain.asp?session=>

# Information Security example:

- Cyber crime enabled by technology - Phishing attacks
  - Trusteer study findings on phishing and banking:
    - Only 0.000564% of bank customers actually click the link in a phishing email.
    - 45% of the people that do click divulge their personal credentials to the fake phishing site.
    - Lots of phishing emails, so about 0.47% of a bank's customers fall victim to a phishing attack in each year
    - <http://www.trusteer.com/sites/default/files/Phishing-Statistics-Dec-2009-FIN.pdf>
  - The criminals collect the information and use it for their own purposes
    - Generally results in financial loss for victims and organisations
    - Estimates range from \$2,400,000 to \$9,400,000 per million bank customers per year.

# Are there information security problems that are not related to the internet?

- Feb 2012 - SunPower Corp theft of IP case
  - US solar panel company
  - Five former employees allegedly stole files from SunPower Corp related to business, including
    - customer contact information and transaction information
    - market analysis
    - business analysis
  - All five former employees now work for rival solar power company
  - Allegedly used USB to steal company files before they left
  - [http://www.cio.com/article/700236/SunPower\\_Lawsuit\\_Highlights\\_Insider\\_Threat](http://www.cio.com/article/700236/SunPower_Lawsuit_Highlights_Insider_Threat)



# Are there information security problems not related to the internet?

- September 2012
  - 3 computers that contained information from the Florida Department of Juvenile Justice reported stolen from an apartment site
  - January 2013 update: At least one was neither encrypted nor password protected and held personal information of over 100,000 youth and employees.
- January 2013
  - Employees accidentally threw out hundreds of patient dental records. These were found by someone looking through a dumpster. Names, Social Security numbers, dates of birth and addresses were exposed.
- Source: Chronology of Data Breaches <https://www.privacyrights.org/data-breach/>

# Outline

- Acknowledgement of Traditional Owners
- Housekeeping:
  - Safety Awareness
  - Code of conduct for lectures
- Introduction to the Unit:
  - Staff
  - Structure
  - Content
  - Assessment
  - Resources
- Why study Security?
- Introduction to Information Security

# Information Security

- OK, we need information security. What's it about?
- Information systems :
  - Collect
  - Store
  - Process
  - Transmit, and
  - Display

data

# Information Security

- What's the difference between information and data?
  - Data is a specific representation of information,
    - so that it can be stored, communicated, interpreted or processed
  - For the data to be useful, you need to understand the representation
    - “There are 10 types of people in the world: those who understand binary, and those who don't.”

# Information Security

- Computers store information as strings of bits, which can be interpreted as different data types
- Common data types:
  - Binary      01000100011000010101010001100001
  - Base ten integer    1147229281
  - Hexadecimal        44615461
  - Real numbers        901.3184
  - ASCII                DaTa
- To view different interpretations of the same 32-bit binary string, try out the Data Representations Applet at <http://math.hws.edu/TMCM/java/DataReps/>

# Information Security

- Information systems involve
  - Property:
    - Physical assets: buildings and contents
    - Hardware
    - Software
    - Data
  - People:
    - Employees
    - Customers
    - Clients
    - Contractors
  - Procedures:
- Need to consider all of these

# Information Security Goals or Services

- Traditional definitions of information security are based on three information security goals or services:
  - **Confidentiality**: preventing **unauthorised** disclosure of information
  - **Integrity**: preventing **unauthorised** (accidental or deliberate) modification or destruction of information
  - **Availability**: ensuring resources are accessible when required by an **authorised** user

# Additional Goals or Services

- These additional goals or services are becoming increasingly important for some applications:
- Authentication:
  - Entity authentication – the process of verifying a claimed identity
  - Data origin authentication – verify the source (and integrity) of a message
- Non-repudiation:
  - create evidence that an action has occurred, so that the user cannot falsely deny the action later



# Information States

- Information security involves protecting information assets from harm or damage.
- Consider information in one of three possible states:
  - Storage
    - Information storage containers – electronic, physical, human
  - Transmission
    - Physical or electronic
  - Processing (Use)
    - Physical or electronic

# Vulnerabilities, Threats and Attacks

- Information security analysis involves considering:
  - Threats:
    - Sets of circumstances with the potential to cause harm by compromising stated security goals
  - Vulnerabilities:
    - Weaknesses in a system that could be used to cause harm by compromising stated security goals
  - Attacks:
    - Occur when vulnerabilities are deliberately exploited
- NOTE: Security incidents can also result from non-deliberate acts.

# Threats, Vulnerabilities and Attacks

## Examples

- **Personal example:**
  - **Threat:** Theft of assets (breach of availability, maybe confidentiality)
  - **Vulnerability:** Poor physical security of site containing asset
    - e.g. unlocked window
  - **Attack:** Burglary
    - e.g. Laptop is stolen
- **Corporate example:**
  - **Threat:** Information assets damaged – breach of availability
  - **Vulnerability:** Physical location of asset
    - e.g. in flood prone area
  - **Event:** Flooding causing damage to property

# Threats, Vulnerabilities and Attacks

## Example: Brisbane floods January 2011

### Furniture men hit roof as computer servers float by

Fran Foo | The Australian | July 05, 2011 12:00AM

A<sup>+</sup> A<sup>-</sup>   Share

 Recommend

 Send

 22 recommendations. Sign Up to see what your friends recommend.

9  retweet

 Share

3



Super A-Mart workers rescuing the company's servers from the Queensland floods. *Source: Supplied*

**THERE** was mud and raw sewage to contend with, but the sight of computer servers floating down a swollen Oxley Creek would have baffled any seasoned angler.

It would also have crippled Super A-Mart's business, already fighting to stem the losses when floods ravaged Queensland earlier this year.

# Threats, Vulnerabilities and Attacks

## Examples

- Corporate example:
  - Threat: Breach of confidentiality of client details
    - e.g. Social security or tax file number revealed to unauthorised user, or credit card or account transaction information
  - Vulnerability: Unprotected storage of client data
    - e.g. Storing files in unlocked room or unsecured database
  - Attack: Attacker observes sensitive client data
    - e.g. Can access credit card number, medical record, account balance
  - NOTE: This may lead to further attacks where the observed information is used

# Threats, Vulnerabilities and Attacks

## Examples

- Corporate example:
  - Threat: Breach of confidentiality of client details
    - e.g. Financial details or medical history revealed to unauthorised user
  - Vulnerability: Not identifying and authenticating sender and receiver of transmissions
    - e.g. Not checking that messages being received are actually from the person/place they claim to be from
    - e.g. Not checking that messages being sent are actually going to the person/place they are intended for
  - Attack: Breach of confidentiality occurs - attacker observes sensitive client data

# Information Security: Attacks

- Two types of attacks:
  - Passive:
    - E.g. eavesdropping, shoulder surfing
    - Attacker's goal is to obtain information
    - Difficult to detect; usually try to prevent the attack.
  - Active:
    - E.g. Phishing, Denial of service, Man-in-the-middle
    - Attacker's goal may be to modify, replicate or fabricate information
    - Difficult to prevent (physical protection may be required)
    - Usual approach is to detect attack and try to recover

# Security Measures or Controls

- Use security measures or controls to counter threats and prevent attacks
  - Also known as countermeasures
- Preventive controls:
  - prevent attempts to exploit vulnerabilities
    - Example: encryption of files to prevent eavesdropping
- Detective controls:
  - warn of attempts to exploit vulnerabilities
    - Example: Use of Checksum/MAC to detect data corruption
- Corrective controls:
  - correct errors or irregularities that have been detected
    - Example: Restoring all applications from the last known good image to bring a corrupted system back online

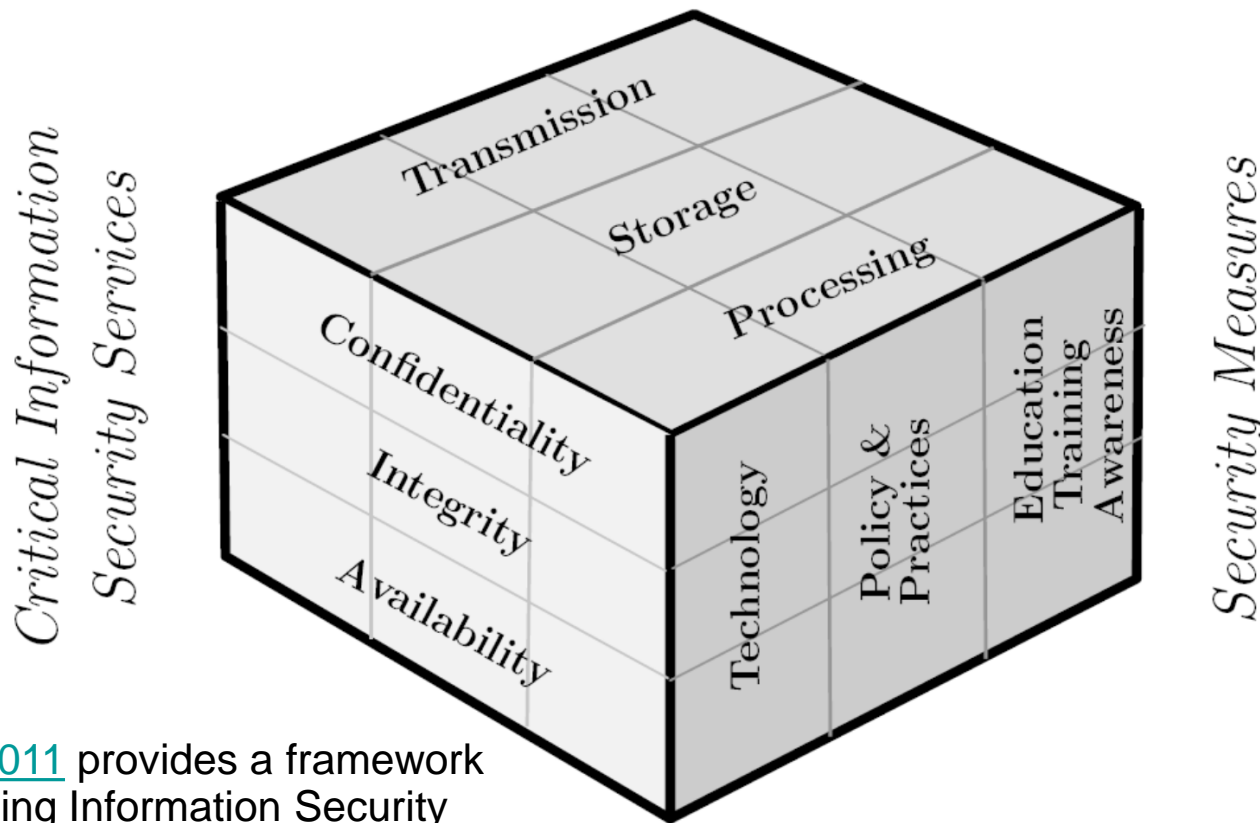


# Security Measures or Controls

- These may involve:
  - Technology
    - Firewalls, Ciphers (encryption), Digital signatures, IDS, tamper-resistant systems, etc
  - Policy and practice
    - Plan outlining organisation's approach to managing information security
  - Education, training and awareness
    - Employee training
      - For example, against social engineering
    - Remember people are components of the information systems

# Useful Diagram: NSTISSI 4011 Security Model

*Information States*



[NSTISSI 4011](#) provides a framework for discussing Information Security

# Summary

- Security is about protecting assets from damage or harm
  - Information is an essential asset, so it needs to be protected
- Traditional information security goals are
  - Confidentiality
  - Integrity
  - Availability
- There are many threats to organizations and their information systems, and many vulnerabilities
- Controls need to be implemented to try to achieve information security goals