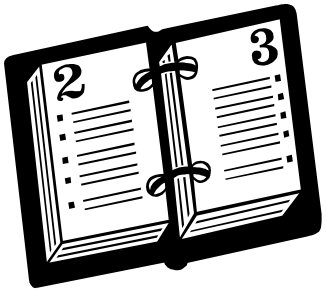
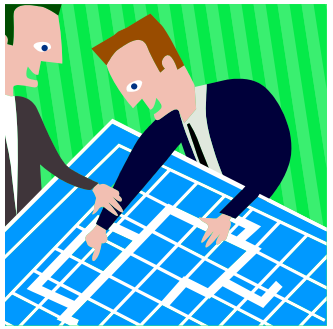
THE UNIVERSITY OF SYDNEY

INFO5990 Professional Practice in IT

Lecture 09A & B





Case studies

Performance testing

Privacy / data

Group Assignment

- Reports to be submitted online on the Sunday
  - **Between 1st May at 11.59 pm till 10th May 11.59 pm (NO EXTENSIONS)**
- **Format – Team name_Assign2.doc**
- **Submission into TurnitIn and Assignment link**
- One person in group to submit both against the team name

==========

- Presentations to be submitted online on the
- Start preparing / practicing
  - **Between 01/05/20 at 11.59 pm to 10/05/20 at 11.59pm (NO EXTENSIONS)**
- **Format: Team name_Assign2.ppt**
- One person in group to submit both against the team name
- No TurnitIn required.

TEAM NAME IS T18C OR T17B ETC

Groups

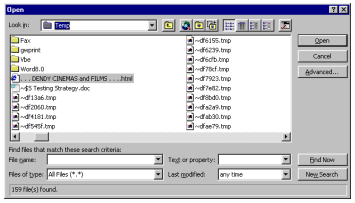
- Make sure you are in the group by now

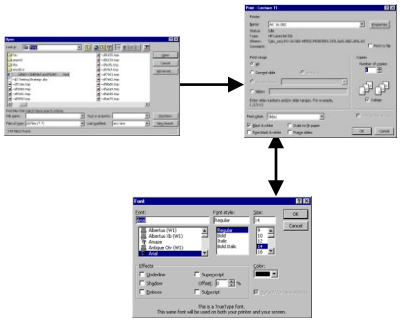
  IN-CLASS ACTIVATION OF GROUPS
- Otherwise you get only 0% when your group may receive HD !
- This is each students responsibility – I cannot check 160+ students
- Please do not come at the end of the term to me if you have not checked your status

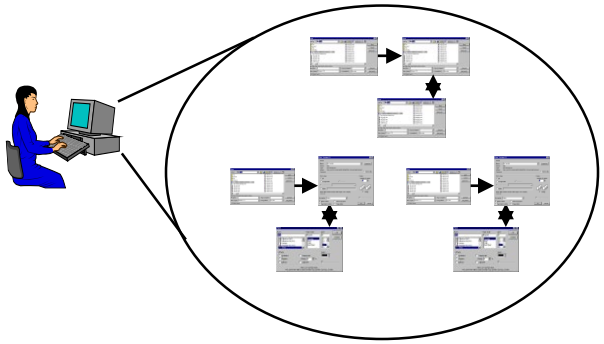
By the end of this lecture you will be able to:

- Appreciate the importance of system testing
- Understand the sort of difficulties encountered in testing large software systems
- Describe the testing arrangements employed in commissioning large software systems
- Case Studies

Testing during development







Component Test

- To ensure that each component behaves ‘correctly’.
- Uses white-box testing to check each program function fully.

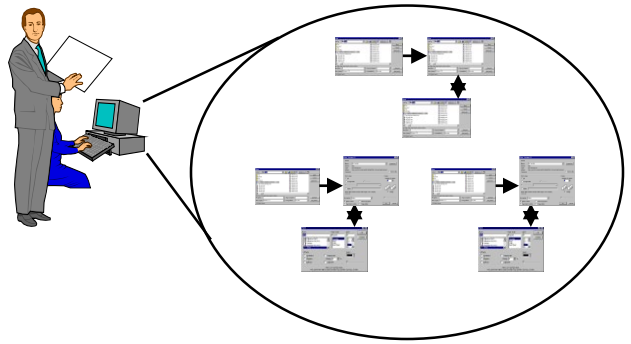
Integration Test

- To test interaction between related components.
- Focuses on interfaces between components.

System Test

- To ensure that the user requirements have been met.
- Focuses on usual business processes, and normal workflow.

Implementation Testing



Performance Test

- To test system performance under maximum expected load.
- Simulates key processes under maximum load.

Soak Test and Stress Test

- To ensure that system is stable over extended period.
- Load increased until system fails. Checks effects of over-load

Acceptance Test

- Compares system functionality against agreed-on user requirements
- Carried out by client using scenarios, supervised by developer

A Bitter experience

‘Nectar’ card launch fiasco

Nectar Fiasco

Tuesday, 17 September 2002

http://news.bbc.co.uk/1/hi/business/2268797.stm

- Customer loyalty scheme, set up jointly by Sainsbury's, BP, Barclaycard and Debenhams: intended to rival ‘Air Miles’ loyalty scheme.
- Offered a reward of 100 points bonus if you registered via internet.

  500 points would get you a ‘Big Mac’!

- As the deadline,17 September, approached millions, hoping to sign up online, found they were locked out.
- They tried, again and again! UNTIL …

The system collapsed!

- Approaching the deadline the website was getting 10,000 hits an hour!
- The sponsors were forced to pull tens of millions of pounds worth of advertising, hundreds of TV spots and press ads.
- *"The online operation was simply taken by surprise by the demand".*
  Ian Barber, Barclaycard

  "All I can think of here is that marketing has not been properly communicating with IT. To send this volume of letters out driving people to the website and not have the capacity in place is a serious flaw".
  Andrew Didcott, Internet expert)

What do you think went wrong?

- The functionality of the system had been tested, but not under load
- Performance testing had not anticipated the level of user load
- Nobody knew that the system would fail completely under pressure
- Was the system testing adequate?

Another testing story

- A global grocery and general merchandising retailer
  - Grocery market leader in the UK
  - 702 stores
  - 30% market share
  - Stores in 14 countries
- In 2002 new online shopping system was to be rolled out
- Management demanded ‘no glitches’
- Other examples:

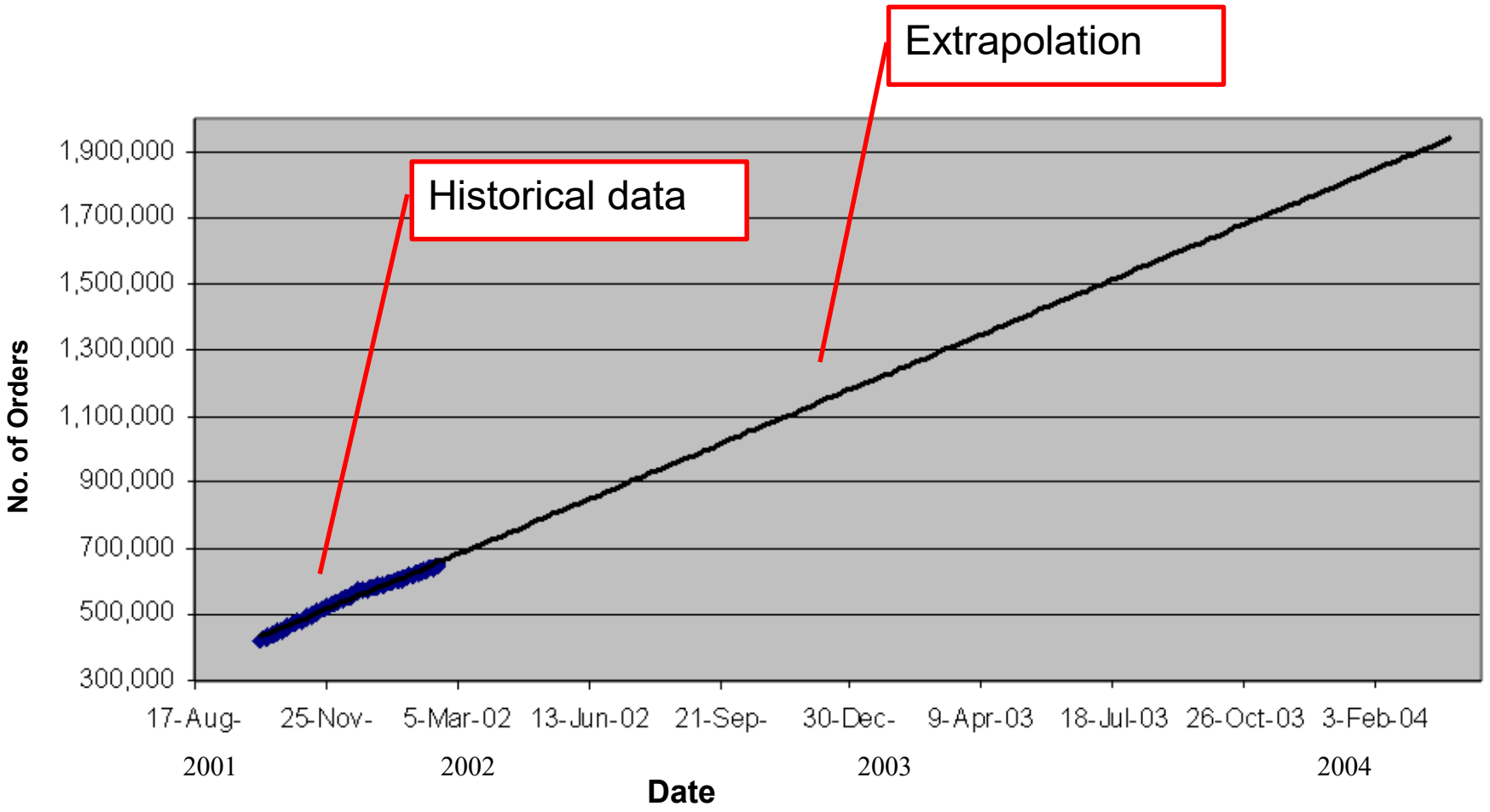
The test plan

- Total budget for testing, £1 million
- Testing to be carried out off line (so as not to interfere with live system)
  - Capacity model: to simulate user load two years into future
  - Usage model: typical mix of tasks
  - Test database: full-sized database, since size affects performance
  - To include soak and stress testing

Test data and test scenarios

Estimating target load

Extrapolating historical data: Oct 2001 – Apr 2002



Determining target load

- Historical data Oct 2001 – Apr 2002
- Trend extrapolated to Feb 2004 gave target 48,655 orders per week
- Corporate plan specified 341,642 orders for final 4 weeks of year = 85, 410 pwk
- +25% for Christmas rush
- +10% for contingency
- *Target load* = 117,439 orders per week

Other examples

- Jetstar 2016

- Australian census 2017

Load test

- Modelling the expected usage of a software program by simulating multiple users accessing the program concurrently.
- Important for multi-user systems, often using client/server model, such as web servers.
- Other examples
  - a word processor or graphics editor could be tested on an extremely large document;
  - a financial package could required to generate a report based on many years' data.
  - A spreadsheet could be tested with maximum columns and rows

Soak Testing

- Testing with a significant load extended over a significant period of time, to discover how the system behaves under sustained use
  - A system may behave as expected when tested for 1 hour, but fail when it is tested for 3 hours.
  - Can expose problems such as memory leaks or stack overflows.
  - Also rounding, accumulation, or compounding errors, which can cause the system to fail or behave unexpectedly after some time.

Stress Testing

Subjecting a system to unreasonable load, while denying it the resources needed to process that load, (RAM, disc, mips, interrupts, etc).

- Stressing the system to breaking point to determine whether the breakdown is potentially harmful.
- Emphasis is on robustness, availability, and error handling, especially when under a load that is heavier than normally expected.
- Will it perform ‘acceptably’ in all situations?
- Particularly important for "mission critical" software, such as medical, space, defence applications
- It is desirable for the system to ‘degrade gracefully’.

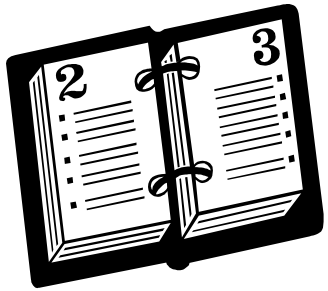
Postscript

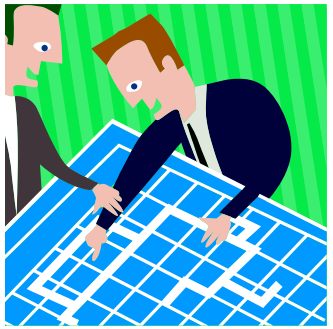
- The Tesco online shopping system has performed without a hitch since it went live in May 2002
- In terms of revenue, Tesco is now third-largest retailer in the world, after Walmart and Carrefour.

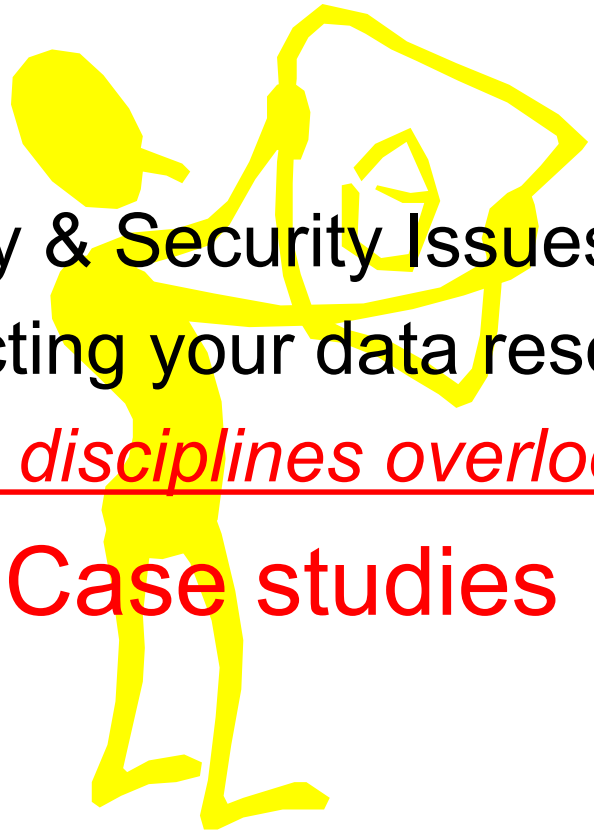
THE UNIVERSITY OF SYDNEY

INFO5990 Professional Practice in IT

Lecture 09B







Privacy & Security Issues in IT

Protecting your data resource

One of the disciplines overlooked in IT

Case studies

By the end of this lecture you will:

- Be aware of the threats to information systems
- Be able to describe some significant cases of security lapses
- Be able to classify and describe common types of attack
- Have formulated your approach to dealing with data security
- And, Bus Continuity
    - And – realise that this is common sense – but ?

The TJX case: 17 Jan, 2007

- TJX retailers
  - 2100 stores in US, 300 in Canada
  - $16 billion annual revenue
- "The worst retail data breach ever?"
  - 46 million customers affected
- Details
  - What happened?
  - How did it happen?
  - What was the result?
  - What lessons?

Timeline of TJX investigation (1)

- 18 December 2006, suspicious software discovered on TJX network
- 17th January 2007 TJX reported unauthorised access to credit card information stored their network
- March 2007 TJX admitted to possible breaches having occurred as early as July 2005
  - Claimed that thieves 'had merely accessed data'
  - Since data was stored unencrypted and held long-term transactions as far back as 2002 could have been affected
  - Potentially 45.7 million accounts compromised.

- Hackers sold 80GB data to thieves
- Fake credit cards used to purchase gift vouchers. Losses experienced by card companies US$8 million.

Timeline of TJX investigation (2)

- Mar 2007 six suspects arrested
  - Irving Escobar, age 18; Reinier Camaraza Alvarez, 27; Julio Oscar Alberti, 33; Dianelly Hernandez, 19; Nair Zuleima Alvarez, 40; Zenia Mercedes Llorente, 23
  - Charged with "organized scheme to defraud"
  - Bonds set at $1 million each.

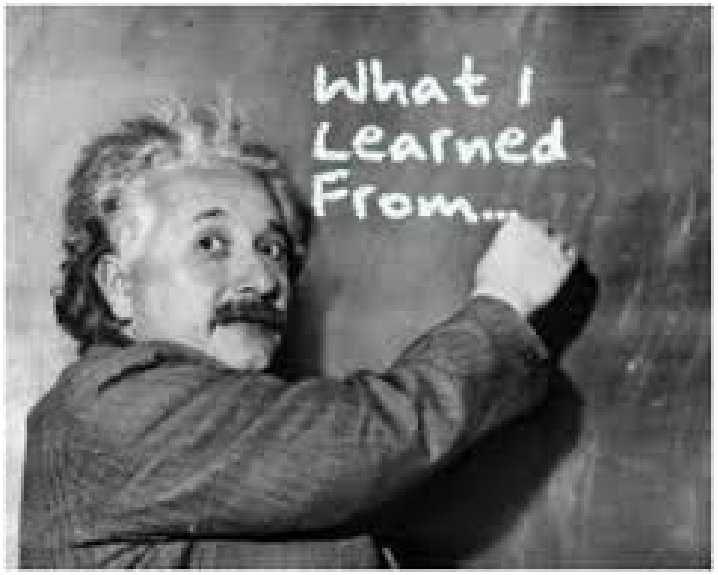
- 8th May 2007 TJX revealed that the fraud had probably been via Wi-Fi. Data was intercepted before it had been encrypted. Thieves also had the key.
- Sept 2007 Irving Escobar sentenced to five years jail
- October 2007 - TJX fined $880,000 by Visa
- November 2007 - TJX settles with Visa for **$40.9M** to cover the costs of reissuing the cards.
- April 2008 – TJX settles with MasterCard for $13M

Aftermath

- August 2008, 11 men charged with hacking into nine U.S. retailers, including TJX.
- March 2010, hacker Albert Gonzalez pleaded guilty. Sentenced to 20 years in prison .
  - the lengthiest punishment ever imposed for computer or identity theft crimes
- 8 May 2010, Ukranian Sergey Storchark arrested in India on his way home.
- 12 April 2011 Albert Gonzalez appealed to have his guilty plea quashed.
  - Claimed he was at the time serving as informant for the Secret Service, and therefore, to be assisting the government , “who had authorized his year’s-long crime spree”.
  - The appeal seems not yet to have been resolved.

What can we learn?

- Need to take care with data
- Data is a saleable commodity – WHY ?
- Follow rules for our own protection
- Criminals are getting smarter
- Consider use of encryption



Australian Computer Crime & Security Survey

Estimated loss to Australia in 2016 due to identity theft and other computer fraud was $5.9 billion. This included:

- Credit card skimming
- Identity theft
- Computer scams
- False passports
- People smuggling
- Money laundering

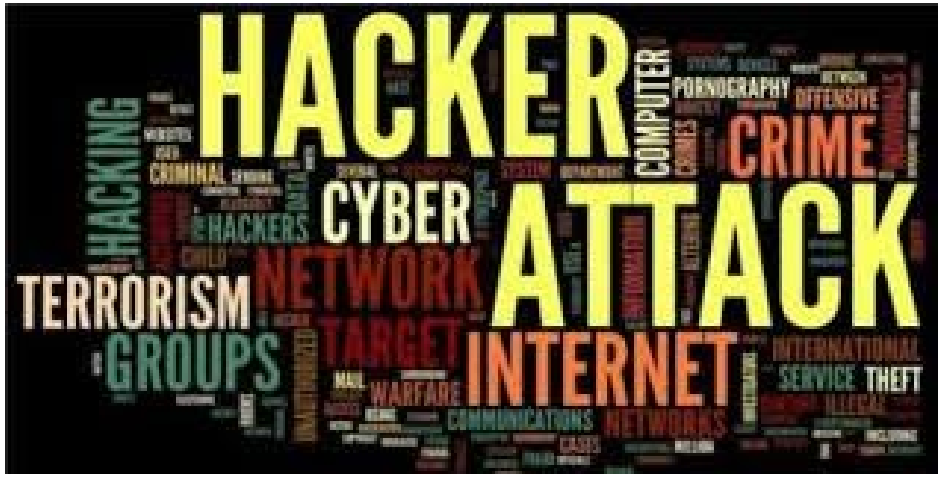
* **A**ustralian **H**igh **T**ech **C**rime **C**entre
†**Aus**tralian **C**omputer **E**mergency **R**esponse **T**eam

Types of crime, abuse experienced

- External attack greatest threat
  - attacked externally, internally.
- Form of crime or abuse
  - insider computer/internet abuse
  - laptop theft
  - virus or worm infection
  - trojan or rootkit attack
  - denial of service/attack
  - unauthorised access
  - computer fraud

Factors thought to contribute to vulnerability

- Unpatched/unprotected software
- Inadequate staff training
- Poor security culture
- Misconfigured software



Aspects of security management that are proving to be a challenge

- Difficulty of changing attitudes of users to security
- Keeping up to date with threats
- Configuration management
- Lack of understanding by senior management
- Lack of commitment by senior management

Cost of computer attacks on Australian organisations in 2016

- Estimated cost
  - Laptop theft $2.3 million
  - Virus, worm attack $960,000
  - Loss of proprietary information* $130,000
  - Denial of service $120,000
- Total annual loss $8.5 million
- Average cost per organisation $240,000

* Plus one respondent who incurred a loss in proprietary information estimated at $40 million

Spending on security by Australian companies

- 66% of respondents reported that they spend between 5 and 10% of IT budget on security
- Software controls
  - Anti-virus software
  - Firewalls
  - Anti-spam filters
  - Security management procedures
  - Media backup
  - System security audit
- Encryption technologies
  - encrypted login/sessions
  - encrypted files

Reporting incidents to law enforcement authorities

- 22% reported the incident
  - 69% of those affected chose not to report – why ?
- Reason given for not reporting
  - Not considered serious enough
  - Didn't think perpetrators would be caught
  - Didn't think authorities were competent
  - Wanted to avoid negative publicity
  - Outcome where reported
  - No charge due to lack of evidence
  - Not investigated
  - Charges laid

Malware as a threat to information security

According to Wikipedia: Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

It can take the form of executable code, scripts, active content, and other software.

The Anti-virus industry

- Examples: Norton, McAfee, Microsoft
  - Symantec Corporation Revenue $6.9 billion, Net income $814 million. Norton Anti-Virus costs $54.99 per year
- The number of potentially malicious threats emerging each month has increased from 300 in 2003 to 4,800 in 2015.
- An unpatched computer with neither antivirus nor firewall protection has a 50 percent chance of becoming a zombie within 30 minutes of being connected to the internet.
  (Sophos, 2006)

Computer crime and the law

What is cyber crime ?

Can we win the fight against cyber crime?

Australian Cases

- In 2005 a Melbourne hacker exposed credit card details of 46,000 accounts.
  - Arrested. Charged with “unauthorised modification of data to cause impairment”.
  - Claimed he was “testing his skills”.
  - Fined $2,000 and had to pay $3,000 compensation to hosting company.
- In 2006 a 17-yr-old student gained access to network of his educational institution.
  - Left message in order to “expose slack system”
  - Arrested. Pleaded guilty. Received a two year good behaviour bond.

Ethical obligations of IT professionals as ‘custodians of information’

Five categories of security threats

1. Unintentional acts
   - Human error, carelessness, ignorance
2. Natural disasters
   - Power outage, fire, flood, earthquake
3. Technical failures
   - Hardware failure, software failure
4. Management failures
   - Ineffective procedures and controls
5. Deliberate acts
   - Vandalism and malicious damage

Protecting data

- Privacy
  - should you store this data?
  - what is it for? is it all necessary?
- Accuracy
  - is it correct, complete and current?
- Property
  - who owns it? can it be sold to others?
- Accessibility
  - confidentiality: who has access to the data?
  - when and for what purpose may it be used?

Factors making security harder

- More complex systems, distributed data, unmanaged devices
- Criminals becoming cleverer: more and more threats
- Crimes often not detected for long periods
- Wide range of users, mostly non-expert
- Management unaware of problems
- Security measures often inconvenient
- Costs substantial
- Benefits hard to quantify

Other major sources of risk

- IT department employees
- Human Resources department employees
- Managers
- Consultants
- Cleaners
- Outsiders, hackers etc
- ‘Social engineering’

The biggest security threat of all:

YOU!!

- Leaving the door open – logged on
- Laptops
  - Over 600,000 laptop thefts occur annually in the US
  - Estimated USD$5.4 billion loss of proprietary information
  - Over 90% of these laptops are never recovered
- Lack of care with passwords
- Opening dodgy emails
  - Test yourself: http://www.sonicwall.com/phishing/
- Careless internet surfing
- Use of portable and unmanaged devices
- Discarded materials and equipment

‘Business continuity’

The last resort:
Backup and recovery

The stark realty

Info Security News Magazine, 2011

- 92% of companies fail to keep their recovery / business continuity plan up-to-date
- An effective DR/BC plan can reduce losses by 90%.
- 88% of e-commerce is not covered by a data recovery/business continuity plan
- 53% of firms recover less than 25% of their total losses through insurance
- 42% of managers do not believe their plans would be effective.

Business Continuity Planning and Management

- Every year 1 in 500 businesses will experience a severe disaster
- 43% of businesses that experience disasters never re-open
- 29% close within 2 years

https://www.youtube.com/watch?v=1V1SCWOXJbc

(Source: McGladrey and Pullen www.continuitycentral.com/feature0660.html)

Business Continuity Management

- Organisation should be able to continue to function during a disaster, rather than simply trying to recover after a disaster has occurred.
- The aim is to come out of an IT mishap relatively unscathed and with little or no impact on your clients or your business.

smh.com.au/articles/2003/10/13/1065917329798.html and
www.johnglenncrp.0catch.com/quotes.html

Classifying business systems

Category	Business requirement
CRITICAL	Functions cannot be performed unless identical (or close to identical) capabilities are found to replace the capabilities affected.
VITAL	There is some tolerance and lower cost to interruption. Functions may be performed by manual means, but only for brief periods of time.
SENSITIVE	Functions can be performed with difficulty, at tolerable cost, manually. But considerable “catching up” may be required once system is restored.
NON-CRITICAL	Applications may be interrupted for an extended period of time, at little or no cost to the organisation, and require little or no “catching up” when restored

Planning for business continuity

- Backup procedures
  - Routine backups
  - Adequate, complete, incremental
  - Mirroring
- Disaster recovery
  - Data, equipment, people
  - ‘Hot’ sites
  - Practice
- System audit

Case Study:
Aust. Stock Exchange
Business Continuity Testing

Participants are advised that from 7 February to 11 February 2016, ASX 24 and ASX Clear (Futures) will be undertaking a comprehensive test of the Business Continuity capabilities of its core systems.

ASX Bridge St core system infrastructure will be configured as standby for redundancy purpose.

Malware as a threat to information security

Last segment – phew!

8 MORE SLIDES TO GO !

Worst attacks of the decade [1]

- 2000 ILOVEYOU (worm)
  - Damage $5.5 to $10 billion.
  - Two young Filipino computer programming students arrested, but released since no appropriate law in the Philippines.
- 2003 SQL Slammer (worm)
  - Damage between $750 million and $1.2 billion.

Worst attacks of the decade [2]

- 2004 MyDoom (worm)
  - $250 million damage, could be as high as $38.5 billon.
- 2004 Sasser (worm)
  - Estimated $500 million damage.
  - 18-year-old Sven Jaschan received a 21 month suspended sentence
- 2009 July cyber attacks (botnet)
  - Major damage. Overwrites data.
  - Attacks on White House and Pentagon.
  - Re-used code from the Mydoom worm.

Malware attacks

- Kinds of attack
  - Denial of service - emails and spam
  - Clandestine acquisition of data - trojans
  - Zero-day attack - specific actions
  - Phishing attack - using email to steal personal data
- Kinds of malicious software
  - Replicating – denial of service
  - Non-replicating – spyware: new trend towards financial gain as motivation

‘Phishing’

- The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
  - The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, and bank account numbers
  - Example (2003) : e-mails supposedly from eBay claiming that the user's account was about to be suspended unless he clicked on the link provided

Is the email really from eBay, or PayPal, or a bank?

As an example, here is what the email said:

- Return-path: <service@paypal.com>
- From: "PayPal"<service@paypal.com>
- Subject: You have 1 new Security Message Alert !

Note that they even give advice in the right column about security

Test yourself:

http://www.sonicwall.com/phishing/

From: "PayPal" <service@paypal.com>
Subject: You have 1 new Security Message Alert !

PayPal

PayPal Security Center: Urgent PayPal Account Login Request.

Notice of account temporary suspension

Dear **PayPal** member :

- We regret to inform you that your **PayPal account**, has been **temporarily blocked** due to various login attempts from different global locations.
- As **Romania** is one of the most high rated fraudulent countries, we temporarily **blocked** your account to avoid future problems or misusage of your **PayPal** account.
- Here are the last 3 login attempts :

How to protect your account

- Make sure you never give away your PayPal login and password. to someone you don`t know.
- Please respect PayPal policy and privacy statements.

For more information on how to protect your account, please visit our security center.
http://www.paypal.com/cgi-bin/cmd=_security-center-outside

Next week's lecture

On presentations and Report Writing

Source: Brightcarbon.com

https://www.fabuss-project.eu/