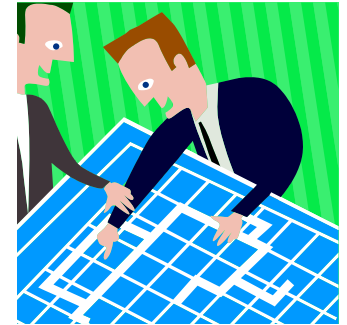




INFO5990 Professional Practice in IT

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

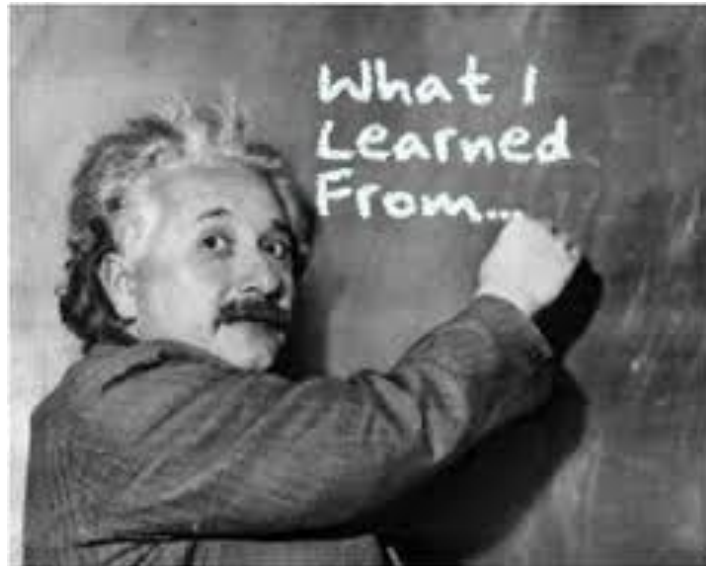
Aftermath

- 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, Ukrainian Sergey Storchak 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



Question 1


Which of the following BEST expresses the prime cause of TJX's mishap?

- A. Management did not care enough
- B. Poor choice of application software
-  C. Weak link in data processing cycle
- D. Failure to have data encrypted
- E. ALL of the above

Question 1	Question 2	Question 3	Question 4	Question 5	Question 6	Score / 6
A B C D E	A B C D E	A B C D E	A B C D E	A B C D E	A B C D E	

Question 2

The most serious problem for TJX resulting from the security breach incident was that:

- A. so much money was involved
- B. the criminals got away with it
-  C. the crime was undiscovered for so long
- D. TJX refused to admit responsibility
- E. credit card companies wanted to sue TJX

Question 1	Question 2	Question 3	Question 4	Question 5	Question 6	Score / 6
A B C D E	A B C D E	A B C D E	A B C D E	A B C D E	A B C D E	

Australian Computer Crime & Security Survey

Estimated loss to Australia in 2014 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

* **Australian High Tech
Crime Centre**
† **Australian Computer
Emergency Response Team**

Australian Computer Crime & Security Survey 2013

- Sample: 2,024 survey forms distributed
- 389 responses received from wide range of organisations (17%)
- 22% of respondents (86) suffered 1 - 5 computer security incidents

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 2012

- 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



Question 3

According to the 2006 AusCERT Survey which of the following statements are FALSE

- A. Loss due computer fraud exceeded \$5 billion
- B. Major reason for not reporting incidents was “not considered serious enough”
- C. Major loss item was laptop theft
- D. Major form of abuse was virus attack
- E. Major difficulty was ‘changing user attitudes’



Question 1	Question 2	Question 3	Question 4	Question 5	Question 6	Score / 6
A B C D E	A B C D E	A B C D E	A B C D E	A B C D E	A B C D E	

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 (2013), 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)

Threat Activity

Recently Discovered


Recently Updated

Name	Type	DAT	Risk	Date Discovered
FakeAV-M.bfr!C71173A7C201	Trojan	6679	Low	13/04/2012
PWS-Zbot.gen.ro!83B9F273F7F7	Trojan	6679	Low	13/04/2012
Generic.dx!06C4E44F9BB4	Trojan	6679	Low	13/04/2012
W32/Chir.b@MM!9A66204A9E6E	Virus	6679	Low	13/04/2012
ErtFor.d!2E9621C49EFA	Trojan	6679	Low	13/04/2012
Generic Dropper.ady!D34285A117DA	Trojan	6679	Low	13/04/2012
Generic.dx!0C3EAE85D0EC	Trojan	6679	Low	13/04/2012
Generic.dx!CD527B00667A	Trojan	6679	Low	13/04/2012
W32/Expiro.gen.h!C7669FDF799A	Virus	6679	Low	13/04/2012
W32/Sality.dr!90A39B67F71C	Trojan	6679	Low	13/04/2012
Vilse!gen.!25955260D744	Trojan	6679	Low	13/04/2012
Generic Dropper!1pn!7894E096D745	Trojan	6679	Low	13/04/2012
W32/Expiro.gen.!1585A4CAD9CF	Virus	6679	Low	13/04/2012
Generic Dropper!7E14DFD9E1B3	Trojan	6679	Low	13/04/2012
W32/Expiro.gen.h!A382F6E2EF43	Virus	6679	Low	13/04/2012
W32/Expiro.gen.h!9ABE45E60CCA	Virus	6679	Low	13/04/2012

The latest crop
of viruses, etc.

Question 4

Which of the following statements relating to malware attacks on computers is FALSE

-  A. Attacks due to malware are becoming less frequent
- B. Rootkit attack is difficult to detect and remove
- C. A trojan appears to be a harmless program, but has other harmful functionality
- D. Melissa was a virus that caused an estimated \$80 million in damage
- E. Code-Red I was an example of a worm

Question 1	Question 2	Question 3	Question 4	Question 5	Question 6	Score / 6
A B C D E	A B C D E	A B C D E	A B C D E	A B C D E	A B C D E	

Computer crime and the law



What is cyber crime ?

Can we win the fight against
cyber crime?

Computer crime and the law

- U.S. Computer Fraud and Abuse Act
 - it is against the law to “knowingly disseminate computer viruses, worms, denial-of-service attacks and other security intrusions”.
- Australia *Cybercrime Act 2001*
(Commonwealth, ACT, NSW, Victoria)
 - Level 1
 - done with the intention to commit a serious offence (i.e. one with a maximum penalty of at least five years)
 - Level 2
 - Impairing or modifying data, or electronic communications, with the intent to cause harm or inconvenience.
 - Level 3
 - Possession, control, production or supply of data with the intent to commit any of the above computer offences
 - Level 4
 - Accessing data that is subject to an access control restriction

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?

Rights of the individual

Court decisions have generally followed two principles:

1. The right of the individual to privacy is not absolute.
 - Individual's rights must be balanced against the needs of society
2. The public's right to know supersedes the individual's right to privacy.

Further ethical questions

- Filtering, monitoring and surveillance
- Social networks
- International aspects
- Profiling

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

Question 5

When considering the capture and storage of personal data, which of the following is NOT an important ethical issue?

- A. Privacy – should it be captured?
- B. Accuracy – is it correct and current?
- C. Property – who owns it?
-  D. Storage – is it stored efficiently?
- E. Accessibility – who is entitled access it?

Question 1	Question 2	Question 3	Question 4	Question 5	Question 6	Score / 6
A B C D E	A B C D E	A B C D E	A B C D E	A B C D E	A B C D E	

'Business continuity'



The last resort:
Backup and recovery
17 Slides to go !

The stark reality

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

(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.johnglennrcrp.0catch.com/quotes.html

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 Monday 7 February to Friday 11 February 2011, 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.



Question 6

Write down
your score

Which of the following factors is important in ensuring business continuity

- A. Establishing routine backup procedures
- B. Practising recovery procedures regularly
- C. Including *people* in the recovery process
- D. Ensuring that all relevant data will be restored
- E. ALL of the above are equally important



Question 1	Question 2	Question 3	Question 4	Question 5	Question 6	Score / 6
A B C D E	A B C D E	A B C D E	A B C D E	A B C D E	A B C D E	

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 billion.
- 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

Replicating: viruses and worms

- Virus can copy itself on a computer without the permission or knowledge of the owner
 - Virus has two key characteristics:
 - Ability to replicate itself
 - Must be attached to another program in order to be executed
- Worm
 - Can execute by itself.
 - Spreads by exploiting security vulnerabilities
 - In 2004 *MyDoom*, infected 250,000 computers in a single day.

'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



Phishing Facts

- 6.1 Billion - Number of phishing e-mails sent world-wide each month
- \$1,200 - Average loss to each person successfully phished (Federal Trade Commission)
- Anti-Phishing Working Group, June 2011
 - 22,273 unique phishing attacks
 - 28,148 phishing Web sites found
 - The country hosting the most phishing sites?
The United States

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 misuse 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

Remember next week is term break

