Joint Universities Computer Centre Limited ("JUCC")

Information Security Awareness Training - Session One

End User Security, IS Control Evaluation & Self-Assessment

Information Security – Trends and Countermeasures

Agenda

- Security News and Trends
  - Data Loss
  - Social Engineering
  - Application Vulnerabilities
  - Organisation Data Leakage and Privacy Infringement

- Countermeasures in Response
  - End User Data Loss Prevention
  - Fighting against Social Engineering
  - Organisation Level Policies and Procedures

NEWS

Data loss through network: Sony's Case

Issue

- Online Entertainment PC games network 'outdated database' was hacked

Date

- May 2011

Consequences

- Personal details of 77 million customers were stolen
- The gaming site, along with Sony's cloud music subscription service was suspended
- Share price of Sony dropped by 4%

Vulnerabilities

- Lack of comprehensive planning and effective monitoring
- Weak security environment designed for credit card database

Data loss through portable media: Western Michigan University lost hard drive containing student information

Issue

- Lost hard drive containing student information

Date

- March 2011

Consequences

- Names and social security numbers of current and former students and faculty members were lost
- Identity theft

Vulnerabilities

- Insufficient controls over general physical security
- Inadequate controls on data backup and restoration

Social Engineering: Using Facebook as a hook

Issue

- Victims received message on Facebook from "friend" inviting them to view a video
- While starting the video, the users were requested to update their computer by downloading unknown software

Date

- July 2011

Consequences

- The downloaded malware elicited active data transfer and stole information from the victims' computer

Vulnerabilities

- Insufficient user education
- Insufficient malware protection

Social Engineering: Lack of Awareness

Issue

- During a security event, calls pretending to be from the IT dept were made to certain large corporations
- Employee were asked to hand over data and visit certain websites

Date

- Aug 2011

Consequences

- Many of the Oracle staff comply willingly, handing over corporate information and visited the websites

Vulnerabilities

- Lack of staff awareness against social engineering

Application vulnerability: Sydney University leaked student details via a web application hole

Issue

- Web application security loophole allowed access to student accounts with no password
- Student information leaked via the web application

Date

- January 2011

Consequences

- Students' personal data were openly available on the Internet

Vulnerabilities

- Lack of systematic monitoring over web applications
- Lack of appropriate testing before production launch

Organisation data leakage and privacy infringement: Local Hospital

Issue

- Clerical staff member of a hospital lost a personal USB flash drive containing one-off data file backup
- No encryption was done when the file was transferred to the USB flash drive

Date

- April 2011

Consequences

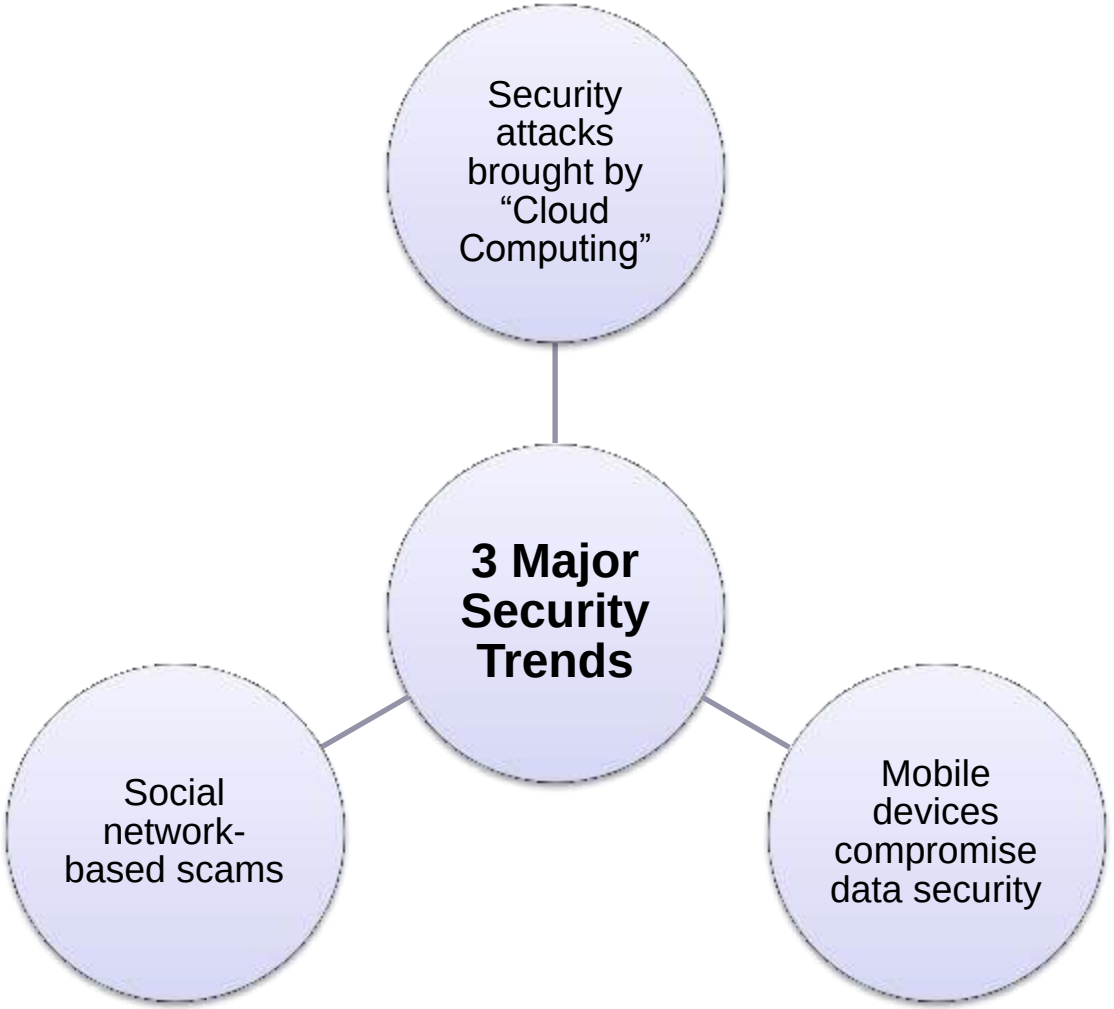
- Names and ID numbers of 19 paediatric patients were lost
- Disciplinary action was taken against the clerical staff concerned

Vulnerabilities

- Lack of data encryption
- Inappropriate use of personal USB flash drive for sensitive data
- Inadequate user information security awareness of sensitive data handling

IT SECURITY TRENDS

IT Security Trends



Security attacks brought by “Cloud Computing”

The Threat

- The majority of cloud computing providers surveyed do not view the security of their cloud services as a competitive advantage
- Cloud computing providers may not consider security as one of their most important responsibilities

How to avoid?

- Ensure **passwords** are properly assigned, protected and changed
- **Gain information about cloud service providers** and other involved third parties which could potentially access your organisation’s data
- **Check reliability** of cloud services and **exception monitoring systems**

Social network-based scams

The Threat

- The most rapid growth in online attacks comes from social networks
- 20% of all Facebook users are active targets of malware
- Cross-site scripting (XSS) and cross-site request forgery (CSRF) vulnerabilities are quickly translating into massive security outbreaks

How to avoid?

- **Do not respond to** any social networking **postings from unknown sources**
- Use of **malware-detection application** (e.g.: “SafeGo” scans user’s account profile for any suspicious links and notify them when a threat is detected)

Mobile devices compromise data security

The Threat

- In Mar 2011, more than 50 third-party applications on Google's official Android Market are discovered to contain a Trojan called DroidDream

How to avoid?

- Avoid installing **mobile OS from unknown source** (e.g. Jailbroken iOS for apple devices)
- Avoid installing any applications from **unknown sources**
- Install mobile **antivirus apps**

1. User runs a mobile app containing Trojan released by hacker
2. Trojan extracts data saved on Smartphone and transfers them to hackers' PC

COUNTERMEASURES

End user data loss prevention

- **Back-up** data files regularly
- **Encrypt** and protect sensitive files with strong password
- Install **anti-malware software** and perform regular security update
- **Understand the risks** associated and the necessary **procedures** before using portable storage devices
- **DO NOT** attempt to **override** controls implemented by IT department

Fighting against social engineering

Common types of social engineering

- **Social engineering by phone**
  - Hackers pretending someone of authority
  - Persuade users into providing sensitive information
  - Impersonate a phone company representative or a bank representative

- **Dumpster diving**
  - A hacker searches for sensitive information (e.g., bank statements, pre-approved credit cards and student loans) in the garbage

Fighting against social engineering

Common types of social engineering

- **Online social engineering**
  - Trick users into providing sensitive information via email or social networking sites
  - Example: A hacker will send a fraudulent email claiming to be a banking institution and request the users to verify their user names and passwords by clicking on a link that directs to a fake website and fill in forms

Fighting against social engineering

Common types of social engineering

- **Social engineering by USB drive**
  - Hackers distribute USB flash memories as souvenir or promotion items
  - These USB flash memories are infected with a virus or Trojan
  - It provides hackers with logins, passwords, and login information of the users' computer

Fighting against social engineering

Against social engineering by phone

- Be skeptical of suspicious calls
- Verify caller’s identity before providing sensitive information

Against dumpster diving

- Shred physical documents
- Sanitise electronic storage media

Fighting against social engineering

Against online social engineering

- Verify the identity of websites before sending over sensitive information
  - Website certificate
  - Known domain name
- Avoid opening and responding to suspicious email
- Centralise reporting of suspicious activities
- Limit information being disclosed

Against social engineering by USB

- Do not use USB devices from unknown source
- Scan USB devices regularly and before use

Organisation level policies and procedures

Preventive measures	Detective measures	Responsive measures
• Educate users about the best practices • Strengthen the security controls	• Monitor network for fraudulent variations • Notify management of suspicious activities	• Establish mechanism to report lost devices • Alert users upon occurrence of security incidents

Security Policy

An effective security policy should be established by the management and IT team, which include the following:

- General guidance on security roles and responsibilities
- Infrastructure security
- Password management
- Procedures for disposal and re-allocation of computing resources
- Data classification and protection
- Incident reporting
- Change management

Summary

- IT Security officer should be kept up-to-date with security vulnerabilities and hacking techniques.
- Consistent assessment of the university's own system and security measures and reporting to management the assessment result is recommended.
- A rigid security policy should be strictly enforced throughout the whole university since data loss can cost the university a significant amount, both in monetary and non-monetary terms.
- Regular user awareness session should be conducted to maintain the awareness of general users.

Q&A

?

Copyright Statement