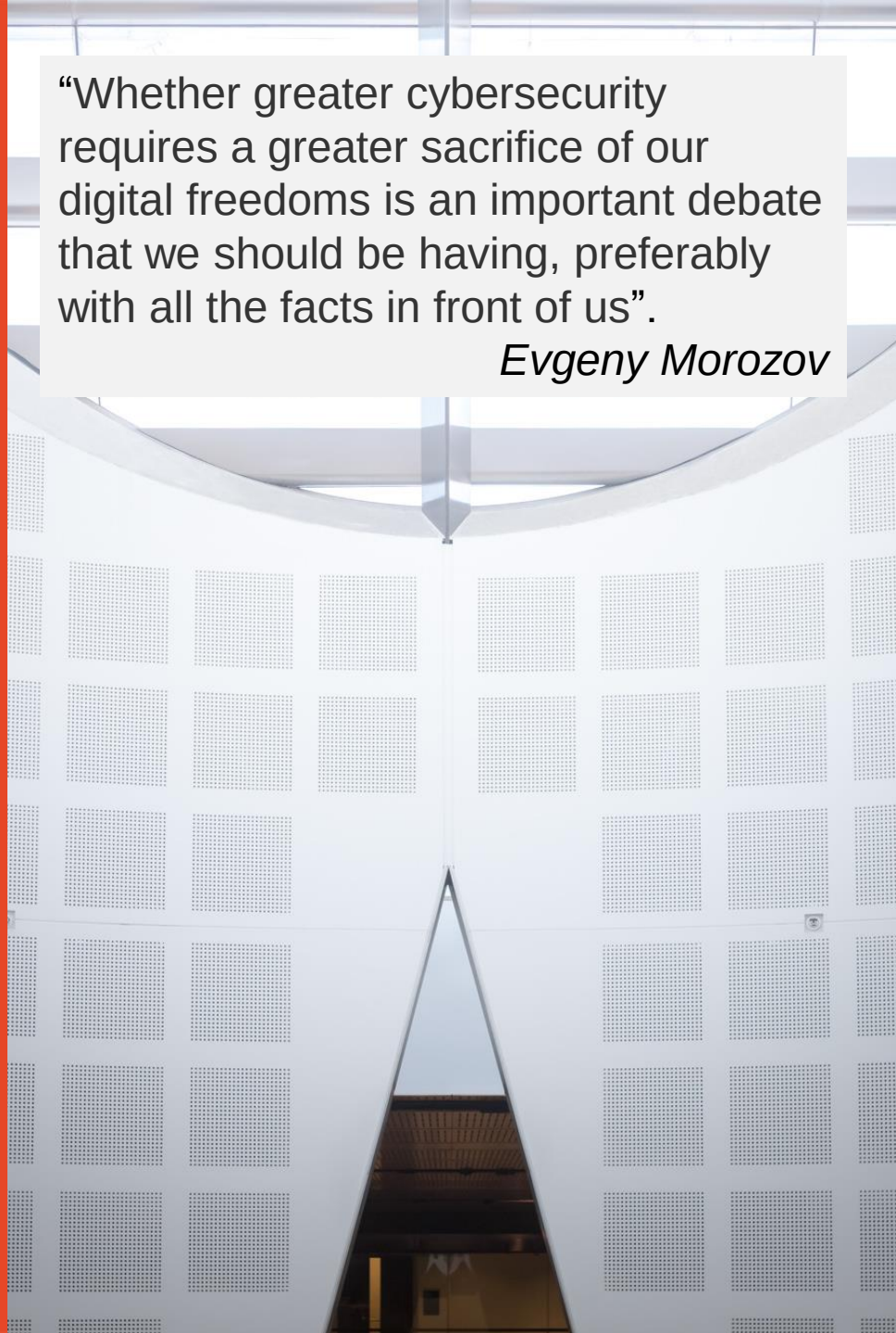
INFO5990: Professional Practice in IT

Week 8: Security Management

Dr. Reza Hoseiny

School of Computer Science

THE UNIVERSITY OF SYDNEY



Overview

- Quiz

- Part A
  - Security Management
  - Not focusing on:
    - Security tools / Techniques
  - Rather, focusing on:
    - Appreciation of the importance of managing security
    - Understand the sort of difficulties encountered in security in large software systems

- Case Studies
- Discussion…

— Chanticleer

The Optus hack will cost millions (and not just in payouts)

Based on the experience of companies overseas, the Optus cybersecurity breach could cost the company hundreds of millions of dollars.

Sep 23, 2022 – 6.54pm

Save Share

The minor move in the share price of Singapore Telecommunications, the parent of cyber-hacked telecommunications company Optus, is surprising given the likely heavy commercial costs from losing the data of up to 9.8 million customers.

Optus will suffer financial damage in two ways. It will lose profits to competitors as existing and potential customers go elsewhere. Also, its expenses will balloon to cover the cost of fixing its weak security defences and to compensate customers.

https://www.afr.com/chanticleer/the-optus-hack-will-cost-millions-and-not-just-in-payouts-20220923-p5bkkm

Security: 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 on 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$50-100 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.

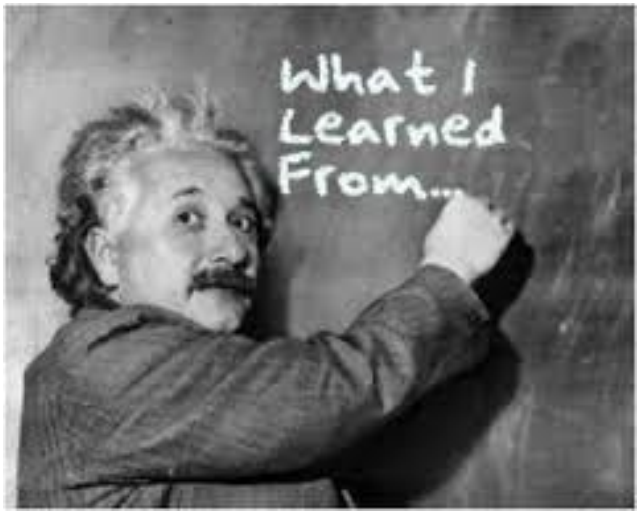
- 8th May 2007 TJX revealed that the fraud had probably been via Wi-Fi. Data was intercepted before it had been encrypted. Thieves also had the key.
- Sept 2007 Irving Escobar sentenced to five years jail
- October 2007 - TJX fined $880,000
- November 2007 - TJX settles with Visa for **$40.9M** to cover 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 filed a motion to withdraw his guilty plea.
  - 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".
  - This was rejected.

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



How big a problem is it?

- See https://securitycenter.sonicwall.com/m/page/worldwide-attacks

Australian Computer Crime & Security Survey

"The Morrison Government estimates cybersecurity incidents cost Australian businesses $29 billion each year. People lost an average of $700 to cybercrimes, according to survey results released mid-2019."

https://www.aic.gov.au/publications/sr/sr43
https://www.emergingit.com.au/insights/the-hidden-costs-of-australian-business-cybersecurity-lapses

- **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

Security Management Frameworks

- ITIL
  - ITIL Security Management
    - https://en.wikipedia.org/wiki/ITIL_security_management
- Cobit
  - APO13: manage security
    - https://miroslawdabrowski.com/downloads/COBIT5/COBIT%205%20-%20Cheatsheet%20%5bv1.0,%20Minimarisk%5d.pdf
    - https://wiki.process-symphony.com.au/framework/lifecycle/process/security-management-apo13-cobit2019/
- NIST Cyber Security Framework
    - https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework
  - 5 functions (comprising 23 categories)
  - Identify (e.g. Business Environment; Risk Assessment; …)
  - Protect (e.g. Access Control; Data Security; …)
  - Detect (e.g. Anomalies and Events; Continuous Monitoring; …)
  - Respond (e.g. Analysis; Mitigation; …)
  - Recover (e.g. Recovery Planning; Improvements; …)

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 2023

- $29 Billion
  - Estimated annual cost to Australian Business from cyber crime
- $276,323
  - Average cost to a business per breach
- 53%
  - Proportion of the cost in detection and recovery
  - (What is the rest?)
- 51
  - Number of days to resolve a ransomware attack

See https://assets.kpmg.com/content/dam/kpmg/au/pdf/2023/cost-of-cyber-attacks-australia.pdf

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

- 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

Data breaches

- See https://www.webberinsurance.com.au/data-breaches-list

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 9,200 in 2020

- 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)

COVIDSafe source code | WFH ur | MyToll still down after ransomwa | Group Presentation, SpeedGrade

ia.acs.org.au/content/ia/article/2020/mytoll-still-down-after-ransomware-attack.html?ref=newsletter

MyToll still down after ransomware attack

Toll Group says it's slowly bringing IT systems back online.

By Casey Tonkin on May 12 2020 10:10 AM

Print article

Logistic company Toll Group is still not fully online following a ransomware attack that brought down its IT systems last week.

In an update yesterday afternoon, Toll said it was bringing its systems "progressively online" after one of its "core IT systems" was securely reactivated last week.

"At the same time, we're continuing to support our large enterprise customers whose services are affected by the disruption to online operations," the company said.

"While there are delays in some parts of the network, freight shipments and parcel deliveries are moving by and large as normal, with Toll call centres taking bookings over the phone."

Toll Group is working through its second ransomware attack of 2020. Image: Toll

Waiting for io.narrative.io...

Type here to search

ENG 5:45 PM 12/05/2020

Computer crime and the law

What is cyber crime ?

Can we win the fight against cyber crime?

Australian Cases

- 1995: Skeeve Stephens
  - Stealing and publishing credit card details
  - 3 years jail
- 2000: Vitek Boden
  - Hacked into Council computers and released millions of litres of raw sewerage
  - 2 years prison
- 2008: Bradley David Ward
  - Hacked into council computers "out of curiosity"
  - Fined.
- 2009: David Anthony McIntosh
  - Hacked NT government systems. $1.2M worth of damage
  - 2 years jail
- 2013: Matthew Flannery ("Aush0k")
  - Numerous hacking offences
  - 15 months home detention
- Various: Julian Assange

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: Users!!

- 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 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

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

Can you think of examples of each?

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.

Worst attacks

- 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.
- 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.

Worst attacks

- 2010: Stuxnet
  - Intended to attack PLCs (Iran nuclear program)
- 2011: LulzSec
  - DDOS hacks
- 2014 : Marriott
  - 500 million accounts
- 2014 : eBay
  - 145 million accounts
- 2016: Adult Friend Finder
  - 412 million accounts
- 2019 : Canva
  - 137 million accounts
- 2020: Sina Weibo
  - 538 million accounts

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 :

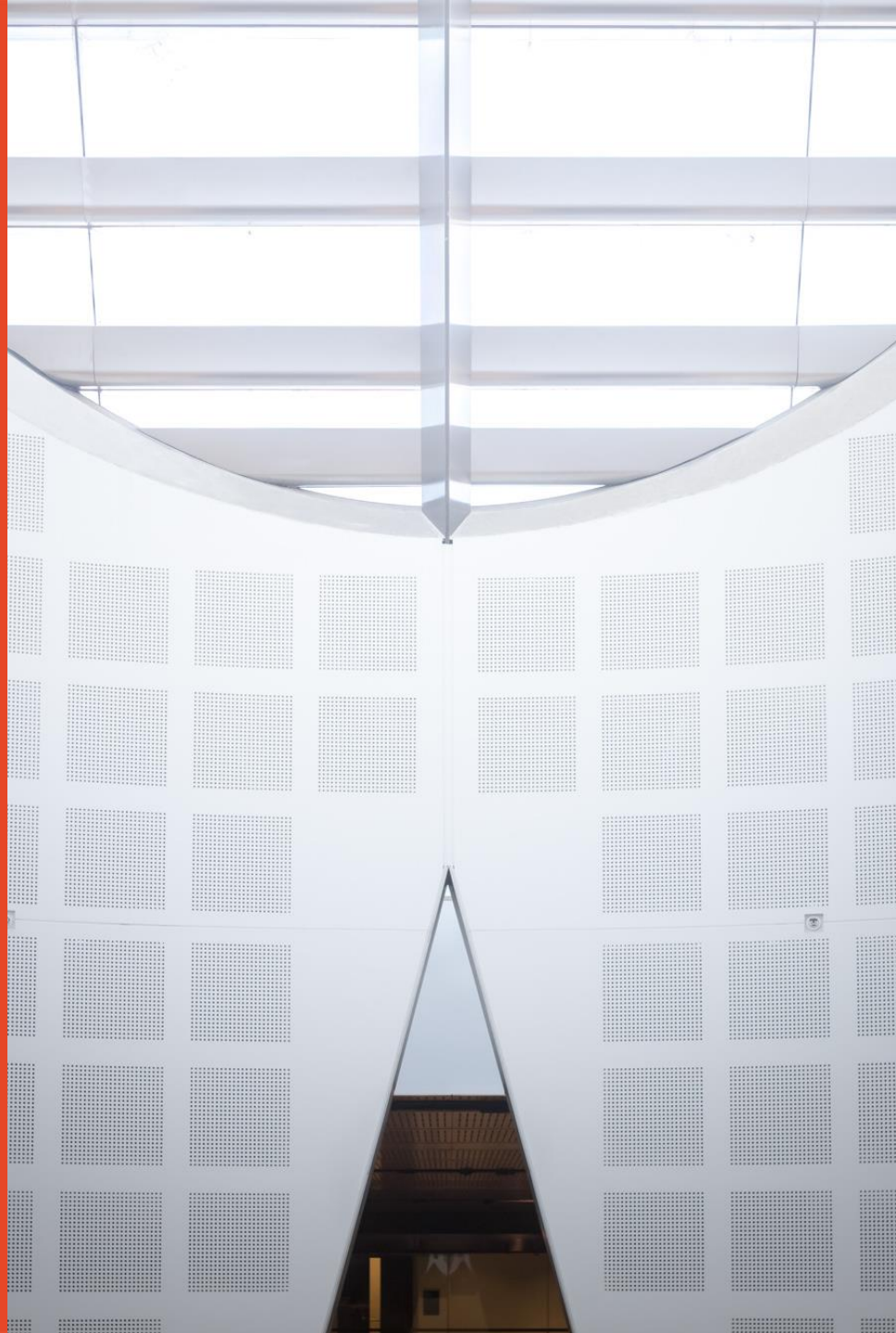
How to protect your account

- 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

INFO5990: Professional Practice in IT

Week 8: Optus…

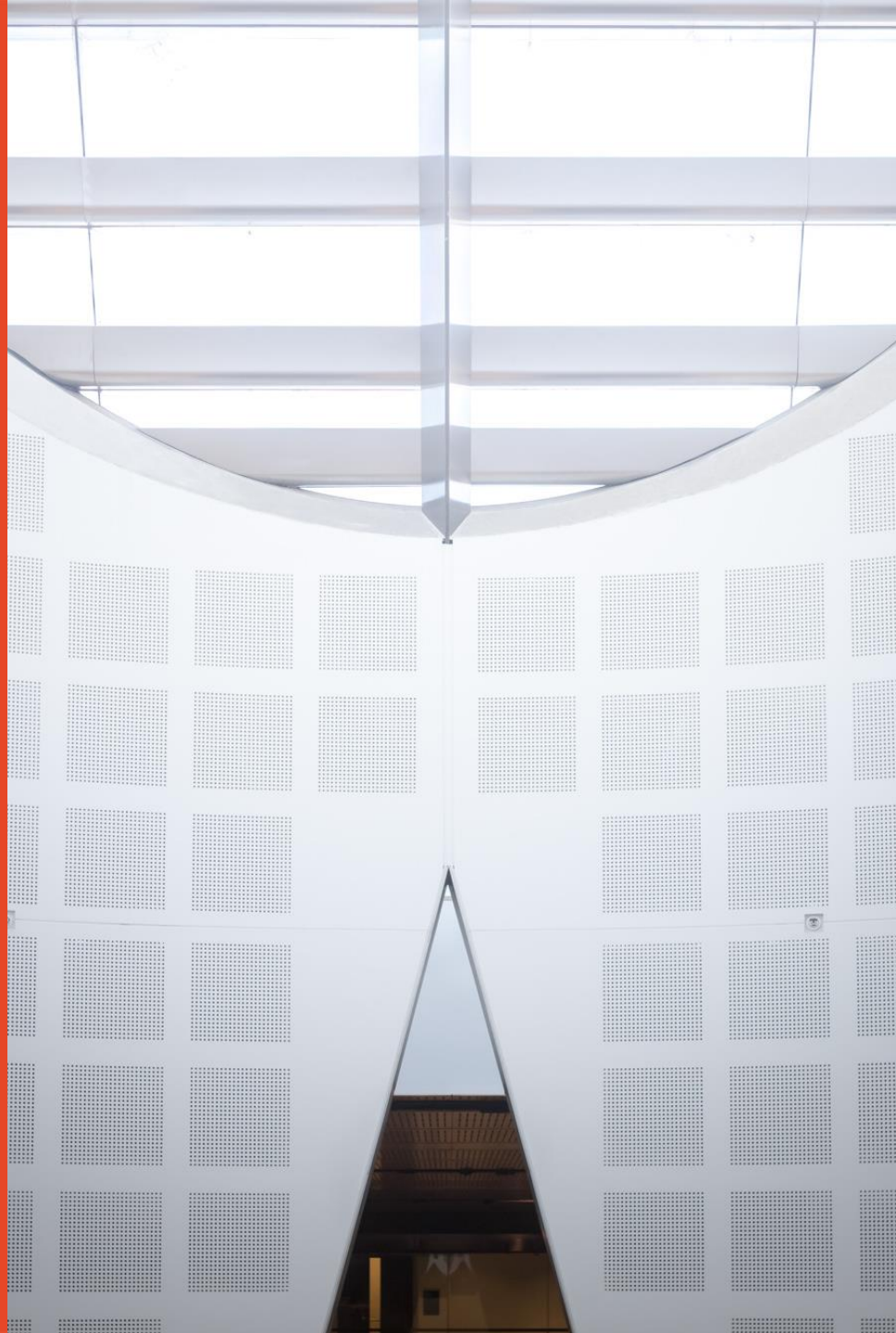


THE UNIVERSITY OF SYDNEY

INFO5990: Professional Practice in IT

Week 8: Discussion

THE UNIVERSITY OF SYDNEY



Questions

1. What are the biggest cyber security threats currently?
2. Who should be responsible for managing security?
3. At what level of a company does this need to be understood?
4. What proportion of a project budget would normally be spent on security?
5. (And on what things would that budget be spent?)
6. Can you be 100% secure?
7. What is meant by:
   - MITM? White-hat? Capture-the-flag? DDoS?
8. What is a pen test?

- https://www.tetradefense.com/cyber-risk-management/15-cybersecurity-questions-to-ask-for-c-suites/
- https://www.guru99.com/cyber-security-interview-questions.html