1

Welcome to INF30020

Slide 2

In this unit, you will be introduced to **information risk and security management** as it applies to **contemporary organisations.** We will be examining the **knowledge and techniques** organisations apply to assessing the risks to their information assets and in so doing, how they provide for improved information security. You will learn about information risk and security management through **real-world case-based scenarios** and become familiar with approaches to **information governance and assurance**.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

2

Welcome

Slide 3

Unit Convener and lecturer

Dr. Paul Scifleet (Lecturer & *primary contact for this Unit)*

pscifleet@swin.edu.au

- Weekly online presentations: usually available on Monday's, preceding Weds classes
- Face to Face classes/ workshops (2hrs) on campus: 8:30am, 10:30am, numbers are limited and you must go to your timetable assigned class
- Consultations: On campus on Monday or Wednesday afternoons, by MS Teams or Zoom at other times, all by by appointment please

Please go to your registered classes.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

3

This weeks learning plan

Slide 4

1. Familiarise yourself the structure of the Unit of Study including,
   - Learning activities, assessment items
   - Class approach and engagement
2. Begin to engage with unit content: Canvas, pre-recorded online lecture, face to face classes and readings
3. Your aim in week 1 is to develop a conceptual understanding of *Information Systems risk and security management* in a global business context and to establish a working knowledge of some key concepts
   - Information Systems Security *and what is at risk* (the information assets of an organisation)
   - Foundation concepts, key characteristics (listed on the final slide)
   - Read, Whitman, Chapter 1

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

4

Summary, schedule and assessment

Slide 5

Week	Week Beginning	Weekly Teaching and Learning	Assessment and Learning activities
1	01 August	Introduction and Overview: IS risk and security	Class activity & reading (TBA)
2	08 August	Information Security & risks I	Class activity & reading (TBA); Submit CLA #1, Friday 11 August
3	15 August	Information Security & risks II	Class activity & reading (TBA)
4	22 August	Assessing security and establishing Internal Control	Class activity & reading (TBA); Submit CLA #2, Friday 26 August
5	29 August	Mitigation, treatment & control I	Class activity & reading (TBA)
6	05 September	Mitigation, treatment & control II	Class activity & reading (TBA); Submit Online Quiz #1, Friday 09 September
Mid Semester Break – 12 September to 18 September. ISRS Report Part A, due Friday 16 September.			
7	19 September	Information Security & Information Governance	Group Warm-up (TBA); Submit in class, Wednesday 21 September
8	26 September	Business Continuity Management	Class activity & reading (TBA);
9	03 October	Contingency Planning	Class activity & reading (TBA); Submit CLA #3, Friday 07 October
10	10 October	Cybersecurity and Business Continuity Management	Class activity & reading (TBA);
11	17 October	Fraud and forensic auditing: Fraud, cybercrime, forensic auditing and continuous monitoring	Class activity & reading (TBA); Submit Report Part B, Friday 21 October
12	24 October	Information Security ethics & compliance and pre-quiz revision	Class activity & reading (TBA); Submit Online Quiz #2, Friday 28 October

Classes

- 1x 40- min pre-recorded lecture posted Monday mornings for review prior to upcoming Weds

  Week 1, introduction pre class
- 1 x 2hr F2F Workshops across the semester, Weds 8:30, 10:30

Assessments

- Continuous learning activities (3 total)
- Individual & group (major) assignment expected release dates at end of week 2 and week 6
- 2 Class quizzes

News

- Guest presentations
  - Program to be confirmed
- ISACA student group
- *All parts of unit of study are relevant to you learning and assessment*

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

5

Unit administration

Slide 6

Schedule and assessment

Types	Individual or Group task	Weighting	Assessment ULOs
Risk and security management report (part A)	Individual Due: 11:59pm, Friday 16 September	25%	1, 2, 3, 5
Risk and security management report (part B)	Group Due: 11:59pm, Friday 21 October; Warm up exercise Weds 21 September.	25%	2, 3, 4, 5
Continuous Learning Activities	Individual (Fridays' at 5:30pm set set weeks, see Canvas schedule)	30%	3, 4, 5
Quizzes (Online)	Individual (6th & 12th week)	20%	1 3, 4

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

6

Swinburne

ISACA®

Trust in, and value from, information systems

Student Group

Business IT meets security!

If you are interested in

- Student community leadership
- Developing a professional career in Information security management and cybersecurity
- Professional career networking
- Being part of the international community of ISACA student chapters

Get in touch and participate

How to Join

Like and Join through our Facebook Page!

@swininfosec or "Swinburne Information Security Society"

SWINBURNE INFOSEC SOCIETY

7

Unit administration

Slide 8

Managing communications and expectations

1. Unit Communication, through classes, canvas, announcements and discussion forums, email, MS Teams or Zoom consultations
   - Only your student account OR Canvas in-system/ clear subject
2. Realistic expectations:
   - Professional and courteous and friendly conduct with peers, colleagues and staff throughout the study period
   - ***Engage, participate (when you can) in class and group discussions***
   - ***Complete weekly required readings and self-directed learning activities***
   - Raise issues with me as they arise, I always aim to respond expeditiously and compassionately
   - Delivery of high-quality, not-plagiarised, not involving cheating work
3. Unrealistic expectations
   - Answering your emails after 5:30pm weekdays and on weekends
   - Requests for last minute extensions (without cause)

8

Unit administration

Slide 9

Referencing and plagiarism: *the rules apply*

1. Referencing is crucial in any university-level assignments
   - Swinburne Harvard Style is required for assignments in this unit
   - See 'Harvard Style Guide' PDF in Resources Folder on Blackboard
2. Know the difference between a Reference List and a Bibliography
   - A Reference List is a list of all the information sources you cite in your work
   - A Bibliography is a list of all the information sources you cite in your work PLUS other sources you have looked at while preparing your work but did not actually use.
   - In this unit you will be asked to produce reference lists for your assignments
3. Please refer to university policy regarding referencing and plagiarism
   - If you are not sure AND/OR want to improve your referencing skills AND/OR want to avoid plagiarism, please ask our librarians

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

9

Unit readings

Slide 10

Required textbook & readings

1. During the semester students are required to familiarise themselves with
   a. relevant Information Security standards for this area of study , including the AGs Protective Security Policy Framework, Australian Government Information Security Manual, *AS/NZS ISO/IEC 27005:2012 : Information technology - Security techniques - Information security risk management*
   b. relevant Risk Management standards and guidelines for this area of study ISO/IEC 13335; **NIST SP 800-30; AS/NZS ISO 31000:2018; HB 254-2005** : Governance, risk management, control and assurance **(**e.g. **ISS 1)**

Recommended introductory reading for week 1 (e-book through library)

Whitman, Michael E. and Mattord, Herbert J. *Management of information security*. Sixth Edition., Stamford, Conn. : Cengage Learning, 2018, **Chapter 1**

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

10

Continuous learning activities

Slide 11

Continuous learning activities (Individual CLAs 30% of marks)

- Are of two types
  A. CLA#1-3 written submissions 10 marks each
  B. <u>Face to Face class activities</u>

<u>F2F Activities:</u> F2F classes each week will involve exercises designed to review all unit content and undertake activities that feed directly into your required learning for assessment tasks.

Weekly learning activities

Slide 12

Weekly learning activities (Individual CLAs 30% of marks)

- Are of two types
  A. <u>CLA#1-3 witten submissions 10 marks each</u>
  B. Face to Face class activities

<u>CLA activities:</u> A 1 page submission ***in Canvas at set weeks*** from week 1 - week 12. There are 3 CLAs, worth 10 marks each, requiring you to answer questions asked about a reading correctly, to demonstration your knowledge with some limited synthesis and some limited analysis involved

CLA#1 is due Friday 12 August

Continuous Learning Activities

Slide 13

How to approach your CLAs

- For each activity, you will be asked to respond to between 1- 4 questions
- Prepare between a half to 1-page written response to the questions identifying key points that answer the question asked
- Marks will be awarded for clear concise answers to the questions asked that demonstrate:
  - Thought, reflection and evaluation in context of the question asked unit learning
  - Draw on relevant unit materials
  - Well-focused and avoiding vague generalisations
- Questions cannot be answered with a simple yes or no but must demonstrate your connection with unit contents
- Marks awarded are based on your answer and your written response

13

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

13

Wednesday's classes 8:30 am and 10:30am

Slide 14

Why not call this unit….

Cybersecurity?

Information Security (InfoSec): the protection of information assets, whether in storage processing or transmission, via the application of policy & procedures, education, training & awareness, and technology …. *Assets and processes*

1. Read Whitman, Chapter 1
2. Undertake a quick Internet search, identify a recent data breach (last 6 months), take brief notes
3. Review CLA#1 in preparation

14

14

Data breach

Slide 15

For class

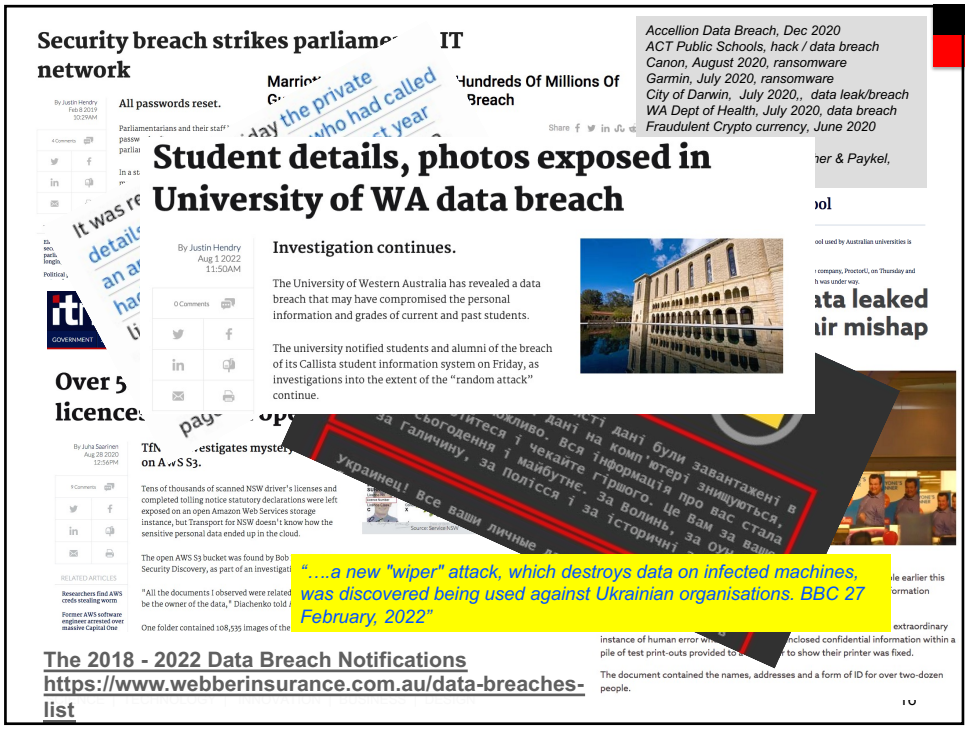
A data breach is

- a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, (disrupted) or used by person/s unauthorised to do so.

- Search the World Wide Web and identify 1x a recent example (***from the last 6 months***) of a **data breach**.

- Examples?

15



Accellion Data Breach, Dec 2020
ACT Public Schools, hack / data breach
Canon, August 2020, ransomware
Garmin, July 2020, ransomware
City of Darwin, July 2020,, data leak/breach
WA Dept of Health, July 2020, data breach
Fraudulent Crypto currency, June 2020

The 2018 - 2022 Data Breach Notifications
https://www.webberinsurance.com.au/data-breaches-list

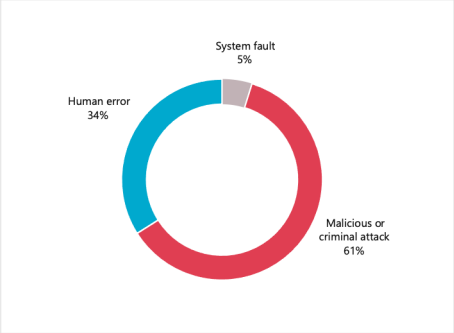
16

Data breach notifications now law

Swinburne

But does it mean things are improving?

"Agencies and organisations regulated under the Australian *Privacy Act 1988* (Privacy Act) are required to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to individuals whose personal information is involved in the breach." Through the *Privacy Amendment (Notifiable Data Breaches) Act 2017* , that came into effect in Feb 2018 and has been operating for 4 years



Source of data breaches — All sectors - Notifiable Data Breaches Report: January–June 2020

Data breach notifications now law

Swinburne

But does it mean things are improving?

"Agencies and organisations regulated under the Australian *Privacy Act 1988* (Privacy Act) are required to notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to individuals whose personal information is involved in the breach." Through the *Privacy Amendment (Notifiable Data Breaches) Act 2017* , that came into effect in Feb 2018 and has been operating for 4 years

Home › News › APS News › Cyber watchdog warns on dark web PS data

APS NEWS

Cyber watchdog warns on dark web PS data

28 January, 2019

The Australian Cyber Security Centre (ACSC) has urged organisations and individuals across the Australian Public Service to check if their email addresses and/or passwords are included on recently released lists of stolen data.

Using the dumped details to remind users of the importance of protecting themselves and their information on the net, ACSC said the released collections contained billions of stolen addresses and passwords and had been sourced from the 'dark web'.

ACSC said it was aware that the so-called Collection #1 dump of stolen credentials had been followed by the release of Collections #2, #3, #4 and #5.

The 773 Million Record "Collection #1" Data Breach: we are now up to #5 and 2.19 billion records

';-- have I been pwnd?

Swinburne

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public. Using the 1Password password manager helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.

Bitly: In May 2014, the link management company Bitly announced they'd suffered a data breach. The breach contained over 9.3 million unique email addresses, usernames and hashed passwords, most using SHA1 with a small number using bcrypt.

Compromised data: Email addresses, Passwords, Usernames

Cit0day (unverified): In November 2020, a collection of more than 23,000 allegedly breached websites known as Cit0day were made available for download on several hacking forums. The data consisted of 226M unique email address alongside password pairs, often represented as both password hashes and the cracked, plain text versions. Independent verification of the data established it contains many legitimate, previously undisclosed breaches. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, Passwords

Data Enrichment Exposure From PDL Customer: In October 2019, security researchers Vinny Troia and Bob Diachenko identified an unprotected Elasticsearch server holding 1.2 billion records of personal data. The exposed data included an index indicating it was sourced from data enrichment company People Data Labs (PDL) and contained 622 million unique email addresses. The server was not owned by PDL and it's believed a customer failed to properly secure the database. Exposed information included email addresses, phone numbers, social media profiles and job history data.

Compromised data: Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Social media profiles

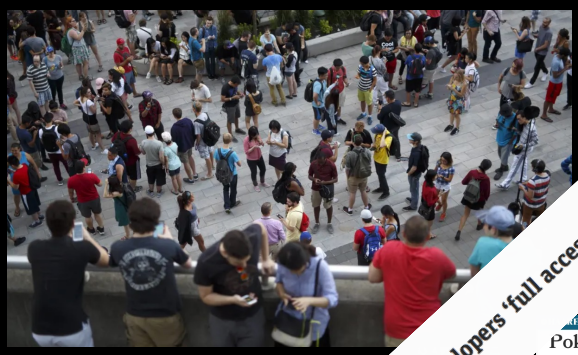
LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Compromised data: Email addresses, Passwords

MyFitnessPal: In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1

19

19



technology

Pokemon Go gives the developers 'full access' to your Google account

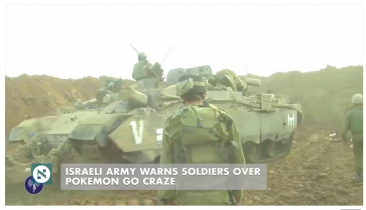
HAARETZ Israel News Jewish World Opinion World News Middle East News U.S. Election 2016

Pokemon Go Craze

The IDF is trying to fight soldiers' use the game, which could allow sensitive information to be posted to the internet.

Gili Cohen | Jul 14, 2016 2:30 PM

Share Tweet 0 Subscribe now



- Pikachu and friends 'drafted' into Israeli army as Pokemon mania sweeps the Jewish state
- To officials' dismay, Pokémon invade Holocaust sites
- Got to catch 'em all: Playing Pokemon in 'real life' not without its dangers

20

Global Cyber security

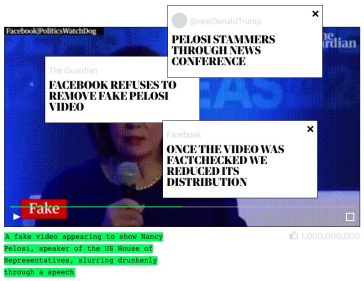
Swinburne

The Watchlist

1. Next Gen network technology,
   - Increasing number of issues around identity and authentication, Zero trust (strict & limited)
   - IoT and urban infrastructure, where and how, what are the most critical elements of infrastructure are and likely to be impacted
   - Deep fakes, existing image or media replaced with a likeness. *Many people view text-based internet communication with skepticism, but what about a phone call from a manager, client, or CEO?*
   - AI and machine learning issues (e.g. risk in areas of health)
   - Hypervigilance, “attack by design” rigorous patterns locating weakness
2. Cyber intelligence and warfare and advanced persistent attacks
3. Space Cyber operations
4. Quantum computing – concerns that can be applied to break encryption

SWIN BUR NE

Slide 22



“Every day now, I start by praying to the data”
https://vimeo.com/437120333

https://www.youtube.com/watch?v=iEZQqsgBPTg

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

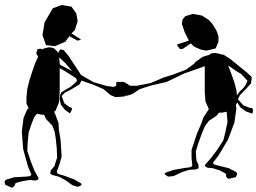
Student Information Security Poll (Straw poll)

Swinburne

Q1: How confident are you about controlling your own information online?

A. Not B. Somewhat C. Comfortably D. Extremely

Q2: Have you been hacked to compromised online? Or know of someone who has?



SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

23

23

What's in a name?

SWIN BUR NE Slide 24

Why not call this unit….

Cybersecurity?

We are are going to be less focused on: Personal security, communication security (in terms of bytes), network security, critical infrastructure security AND most focused ***on Information Security …….in organisational contexts: InfoSec***

The prevention of damage to, unauthorized use of, exploitation of, and, if needed, the restoration of electronic information and communications systems (and the information contained therein) to ensure confidentiality, integrity and availability [of information & information services].

U.S. National Infrastructure Protection Plan, 2005

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

24

24

1. Importance of ISRS to business

Slide 25

Prelude – global transformation

The integration of business and technology has allowed organisations to transform the way they conduct themselves; to become more efficient and effective; to increase share; and to increase their participation in the global economy

It is this complex, interacting system of technology and organisational processes underlying economic growth and social change that we need to begin to think differently about: its not just the way that we buy & sell things that has changed it is our ***mode of development: informational*** (Manuel Castells)

- Let's think about this in terms of the continuum of corporate information (*or, for that matter – our personal information world*)
- **Digital assets;** human communication, knowledge sharing and business intelligence, IOT, production processes and industry 4.0

25

Swinburne

Australian Cyber Security Centre (ACSC) Cyber Security Survey, 2017

(Survey results for 2015-2016)

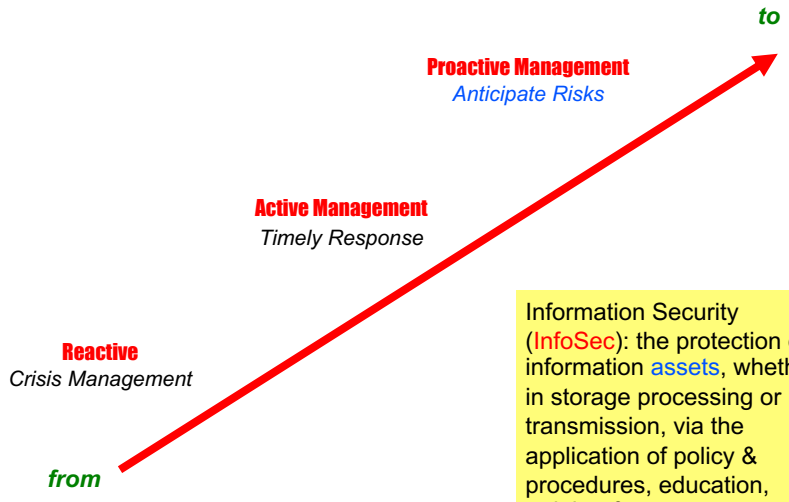
113 organisations completed the survey in 2016, including 68 private sector and 45 government organisation

...71% of organisations report having a cyber security incident response plan in place...

29% don't!!

26

Proactive InfoSec



Information Security (InfoSec): the protection of information assets, whether in storage processing or transmission, via the application of policy & procedures, education, training & awareness, and technology *…. Assets and processes*

27

1. Importance of ISRS to business

Slide 28

Information assets

- Information is a **valuable** business asset creating the primary objective of the information security team "*protect information assets*" (Whitman page 3)

define…

- *What* information needs to be protected?
- *Why* it needs to be protected?
- *What* happens if it is not protected?
- Virtual assets compared to physical assets
- Knowledge assets & intellectual property
- What are the most significant assets to an organisation?

An information asset: any information resource valued by the organisation as such; e.g. data, device or component of the information environment; information and related resources .. Including people

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

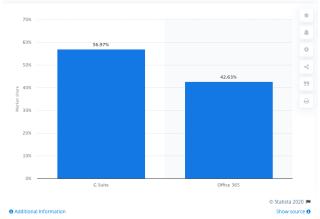
28

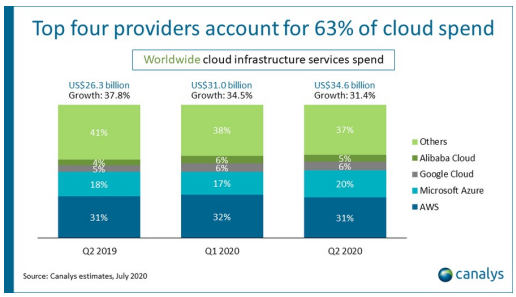
1. Importance of ISRS to business

Slide 29

Information processes (*communications & functions*)

1. What information handling takes place? e.g. communication and storage of payment card details
2. What information / data services are involved? e.g. outsourced Cloud services for storage
3. What corporate functions are e.g. Google corporate mail services,





Google G suite now holds 56.97% of U.S office suite market share

29

1. Importance of ISRS to business

Slide 30

What is risk?

- Simply put, we might say that risks are the price of doing business, they are the chances of negative outcomes
- A risk is the potential that an organisational asset in use use or of value will be compromised
- From our family of security standards, a risk is:

  The potential that a threat will exploit a vulnerability *of an asset or group of assets* and thereby cause harm to the organisation (…..i.e. have an impact)

ISO/IEC 27000: Information Security Management

30

1. Importance of ISRS to business

Slide 31

Controlling for risk?

- We can manage for risk by establishing **controls**
- Information Security Management (ISM) is about establishing controls (usually internal … approaches to managing for risk)
- Its the *absence* or *weakness* of control that creates our **exposure** (to risk)
- It is the vulnerabilities in the **internal controls** organisations put in place that can expose them to:
  1. Destruction of assets (physical & information)
  2. Theft of assets (physical & information)
  3. Corruption of information or the information systems
  4. Disruption of the information system

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

31

2. Information Systems Security

Slide 32

What is security?

1. Security is: (some samples from: wordnet.princeton.edu)
   - the state of being free from danger or injury
   - defense against financial failure; financial independence
   - freedom from anxiety or fear
   - a formal declaration that documents a fact of relevance to finance and investment
   - property that your creditor can claim in case you default on your obligation
   - a department responsible for the security of the institution's property and workers
   - a guarantee that an obligation will be met (surety)
   - an electrical device that sets off an alarm when someone tries to break in
   - measures taken as a precaution against theft or espionage or sabotage

2. We can take from this the idea that information security is essentially the mechanisms (controls, processes & procedures) we put in place to protect or organisations and their information assets against threats: securing the resources that we value

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

32

2. Information Systems Security

Slide 33

What is information security?

"Information security involves protection of information assets (whether in digital, physical or human form) and information systems from damage, misuse or attack (whether in storage, processing, or transit), resulting in information being stable, reliable, and free of failure."

(Source: Bihari, E. 2003, Information Security Definitions, www.perfres.net)

Preservation of **confidentiality, integrity and availability** of information; in addition, other properties such as authenticity, accountability, non-repudiation can also be involved (ISO 27001:2006)

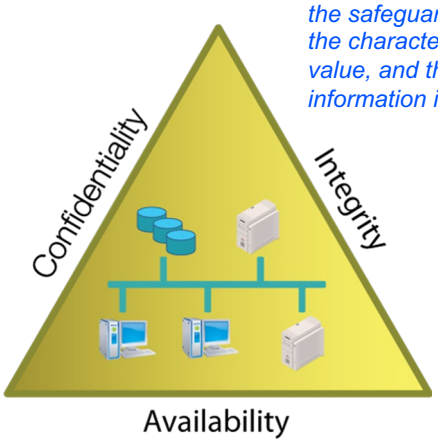
33

2. Information Systems Security

Slide 34

Starting point, addressing CIA

Information security (InfoSec) is the safeguarding of information, the characteristics that give it value, and the means by which information is secured



Whitman paraphrased, page 5

34

2. Information Systems Security

Slide 35

Confidentiality, Integrity, Availability

1. ***Confidentiality is limiting access only to those who need it***; it is about restricting of access to certain types of information to authorized individuals with proper permission

   e.g. the loss of credit card information could be considered a breach of confidentiality / access control mechanisms support confidentiality, e.g. cryptography, passwords

2. ***Integrity refers to the trust worthiness of the information*** or the support IT resources. It covers both the content of the information and the origin of the information. The preservation of data in an uncorrupted stated

   e.g. altering digital records (financial transactions) could be considered a breach of integrity, faulty transmission,/ prevention control mechanisms support integrity by blocking unauthorised attempts to change data, detection mechanisms report that the data's integrity may no longer be trustworthy

3. ***Availability of the information and the ability to use the information*** or supporting IT resources as desired

   e.g. a denial of service attack could be considered a breach of availability / establishing a control environment through continuous monitoring can be used to support availability

2. Information Systems Security

Slide 36

Information security and threats

Threats defined ….

Anything that is capable of acting in a manner resulting in harm to an asset *and/or organization; for example, acts of God (weather, geological events, etc.); malicious actors; errors; failures. (The Open Group)*

With threats that include

- Hackers, intentionally accessing a system without authorisation
- Disruption or prevention of operations (DOS/D-DOS attacks)
- Malicious software (Android/Spy.Agent.SI) viruses (NIMDA)
- Snooping, unauthorised interception of information
- Modification and alteration, masquerading
- Delay, Denial of receipt, repudiation of origin
- Spam
- Criminal purposes, credit card theft, identity theft, sabotage, espionage, extortion, fraud
- *Systems failure, human error, loss of privacy and confidentiality*

2. Information Systems Security

Slide 37

Data breach

A data breach is

- a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, (disrupted) or used by person/s unauthorised to do so.
- may involve financial information such as credit card or bank details, personal health information, other personally identifiable information (including the loss of privacy) trade secrets of corporations or intellectual property.

- …and in preparation for Week 2: please watch this video in your own time: Target data breach: https://www.youtube.com/watch?v=pom42RDo_wE

Data breach

Swinburne

Short reading: Bunnings exposed staff performance .....(Canvas)

Q1: In terms of Information Security and the 2019 Bunnings data breach, which of the following 3 areas of security is most significant? Why?

(a) Confidentiality, (b) Integrity, (c) Availability.

1. **Confidentiality is the restriction of access to certain types of information only for authorised individuals with proper permission**
2. **Integrity refers to the trust worthiness of the information or the support IT resources. It covers both the content of the information and the origin of the information. The preservation of data in an uncorrupted stated**
3. **Availability of the information and the ability to use the information or supporting IT resources as desired**

Data breach

Swinburne

Short reading: Bunnings exposed staff performance database

Q2: What view do you take about company 'reputational risk' when it comes to data breach

(a) They should minimise news about the extent of the breach. Why?

(b) They should reveal everything about the breach. Why?

39

Data breach

Swinburne

For next week's class

Search the World Wide Web and identify 1x a recent example (***from the last 6 months***) of a **data breach**.

- What is a data breach? Describe the characteristics of your example the data breach (How did it occur and what was most siginifcant about it?)
- What are the implications and lessons learnt from this data breach?
- *what was the main threat and are the most important lessons for you …..in terms of CIA especially*

A threat: Anything that is capable of acting in a manner resulting in harm to an asset and/or organization; for example, acts of God (weather, geological events, etc.); malicious actors; errors; failures. (The Open Group)

40

Data breach

Swinburne

For next week's class

A data breach is

- a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, (disrupted) or used by person/s unauthorised to do so.

…and in preparation for M002/Week 2: please watch this video in your own time: Target data breach:
https://www.youtube.com/watch?v=pom42RDo_wE

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

41

Thank you

SWINBURNE UNIVERSITY OF TECHNOLOGY

Questions

Terms for week 1

1. Information Systems ***Risk*** and ***Security … importance of internal control*** , *an InfoSec definition of risk*
2. The CIA (***Confidentiality***, ***Integrity***, ***Availability***)
3. **Other key terms from week 1:** ***Information asset, risk, control,Infosec, data breach, threat, vulnerability, malware***

Swinburne think forward

42