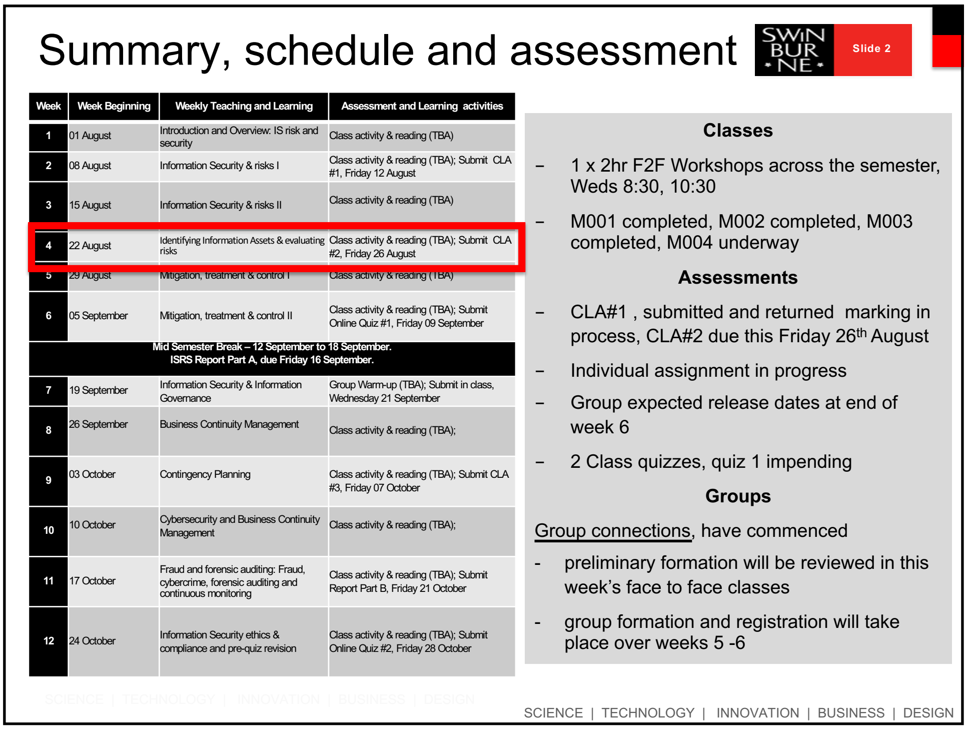
Welcome to INF30020 Module 4: Identifying Information assets and evaluating risk

In our F2F classes this we will work closely with the eTricity Case Study, have you read it yet?

SWINBURNE UNIVERSITY OF TECHNOLOGY
ADVANCED TECHNOLOGIES CENTRE
Swinburne
think forward

1



Summary, schedule and assessment

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 12 August
3	15 August	Information Security & risks II	Class activity & reading (TBA)
4	22 August	Identifying Information Assets & evaluating risks	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

- 1 x 2hr F2F Workshops across the semester, Weds 8:30, 10:30
- M001 completed, M002 completed, M003 completed, M004 underway

Assessments

- CLA#1 , submitted and returned marking in process, CLA#2 due this Friday 26th August
- Individual assignment in progress
- Group expected release dates at end of week 6
- 2 Class quizzes, quiz 1 impending

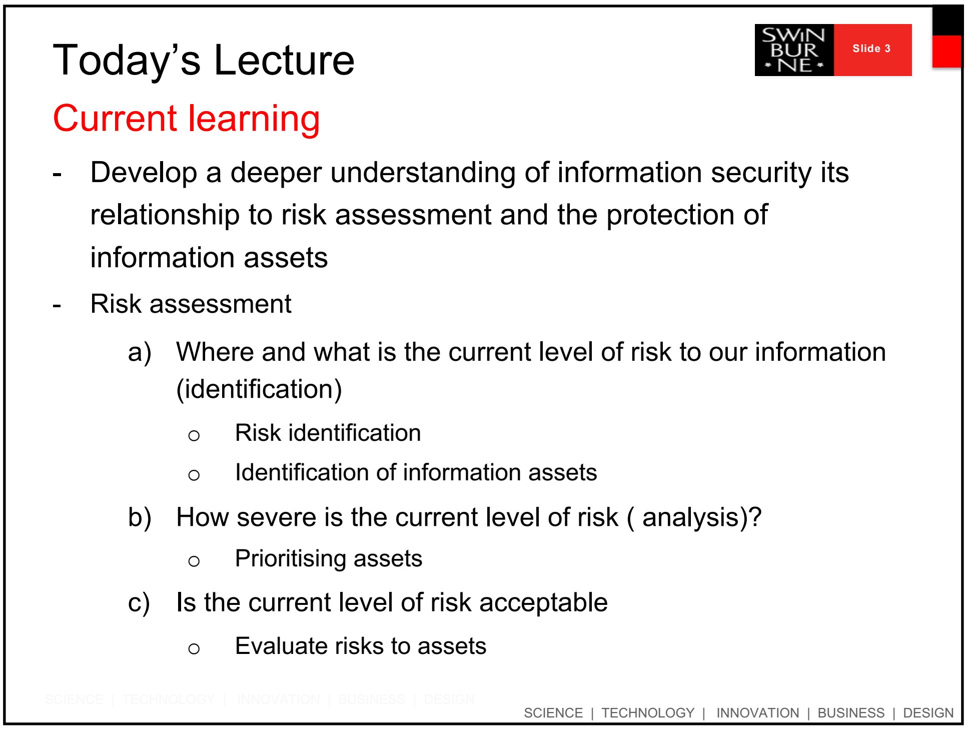
Groups

Group connections, have commenced

- preliminary formation will be reviewed in this week's face to face classes
- group formation and registration will take place over weeks 5 -6

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

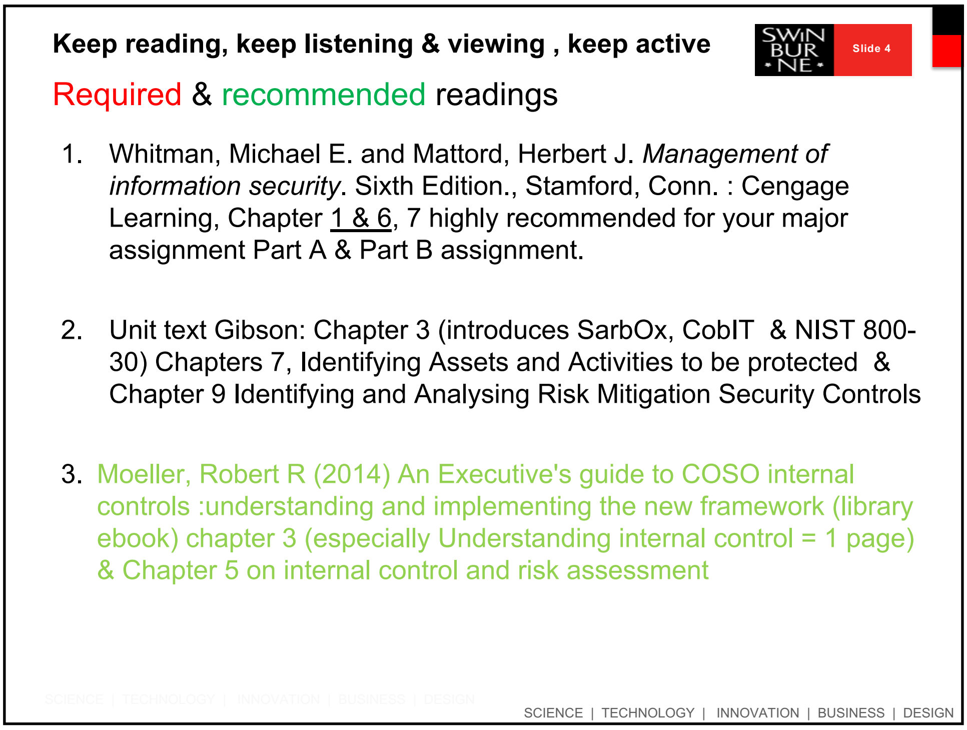
2



Today's Lecture

Current learning

- Develop a deeper understanding of information security its relationship to risk assessment and the protection of information assets
- Risk assessment
  - a) Where and what is the current level of risk to our information (identification)
    - ○ Risk identification
    - ○ Identification of information assets
  - b) How severe is the current level of risk (analysis)?
    - ○ Prioritising assets
  - c) Is the current level of risk acceptable
    - ○ Evaluate risks to assets



Keep reading, keep listening & viewing , keep active

Required & recommended readings

1. Whitman, Michael E. and Mattord, Herbert J. *Management of information security*. Sixth Edition., Stamford, Conn. : Cengage Learning, Chapter 1 & 6, 7 highly recommended for your major assignment Part A & Part B assignment.

2. Unit text Gibson: Chapter 3 (introduces SarbOx, CobIT & NIST 800-30) Chapters 7, Identifying Assets and Activities to be protected & Chapter 9 Identifying and Analysing Risk Mitigation Security Controls

3. Moeller, Robert R (2014) An Executive's guide to COSO internal controls :understanding and implementing the new framework (library ebook) chapter 3 (especially Understanding internal control = 1 page) & Chapter 5 on internal control and risk assessment

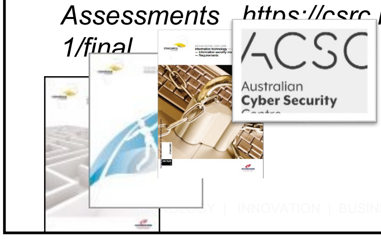
Keep reading, keep listening, keep active

Required Standards (the expectation is that they are included)

AS ISO 31000:2018 : Risk management – Guidelines http://ezproxy.lib.swin.edu.au/login?url=https://subscriptions.techstreet.com/products/806031 e.g. section 5.4.3 discusses assigning roles, responsibilities and authorities on page 7

AS/NZS ISO/IEC 27005:2012 : Information technology - Security techniques - Information security risk management [http://ezproxy.lib.swin.edu.au/login?url=https://subscriptions.techstreet.com/products/862854 (Links to an external site.)](http://ezproxy.lib.swin.edu.au/login?url=https://subscriptions.techstreet.com/products/862854)

NIST 800-30 r1, Guide for Conducting Risk Assessments https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final



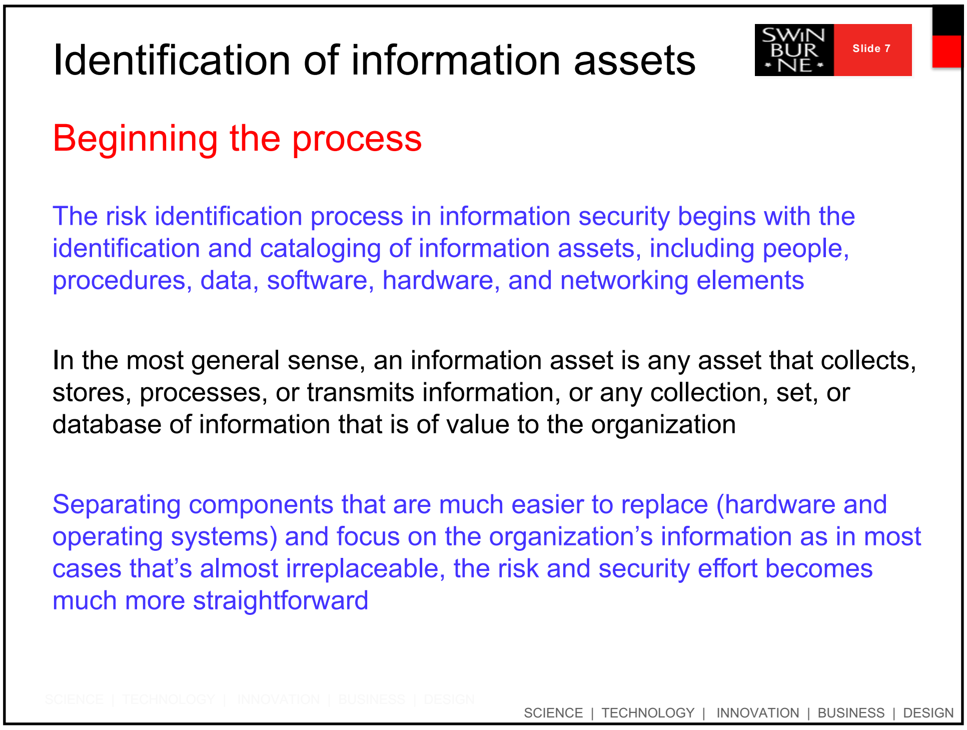
Information Assets and Business Requirements (2011). The National Archives of the United Kingdom

Today’s Webinar

Current learning

Concepts to cover in your learning

- The steps in Information risk assessment (*ISO 31000, AS/NZS ISO27005)*
  - Identify risks
  - Analyse risks
  - Evaluate risk
  - (assess assets, threats & vulnerabilities, e.g. like OCTAVE)
- *COSO ERM framework*
- Information Security
- Internal Control frameworks
- PDC in Internal Control



Identification of information assets

Slide 7

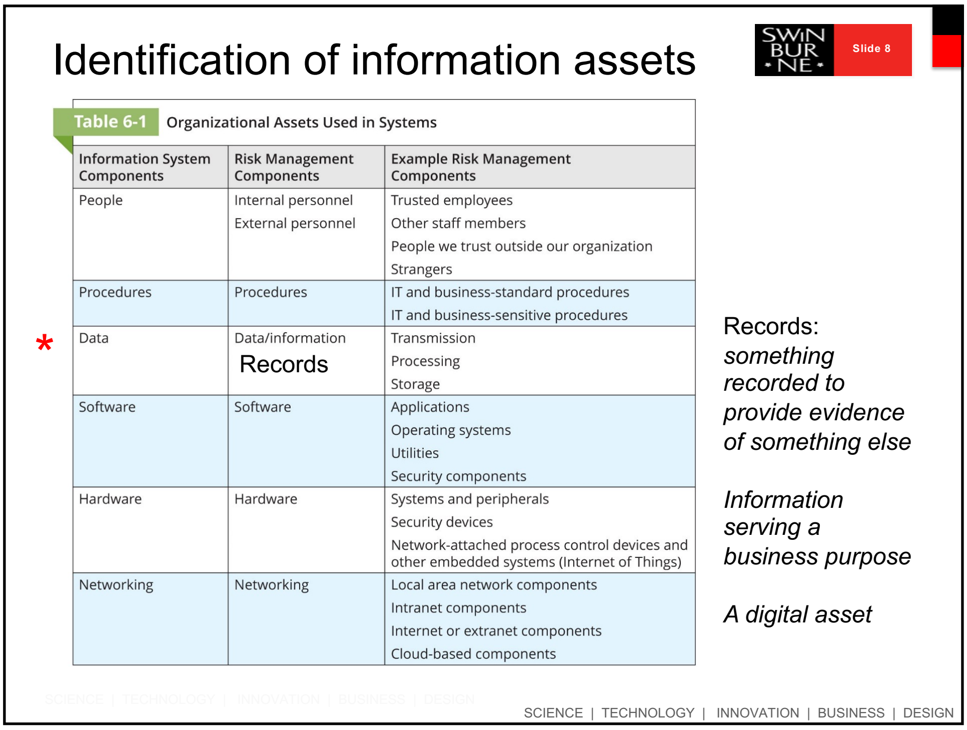
Beginning the process

The risk identification process in information security begins with the identification and cataloging of information assets, including people, procedures, data, software, hardware, and networking elements

In the most general sense, an information asset is any asset that collects, stores, processes, or transmits information, or any collection, set, or database of information that is of value to the organization

Separating components that are much easier to replace (hardware and operating systems) and focus on the organization's information as in most cases that's almost irreplaceable, the risk and security effort becomes much more straightforward

7



Identification of information assets

Slide 8

Table 6-1 Organizational Assets Used in Systems

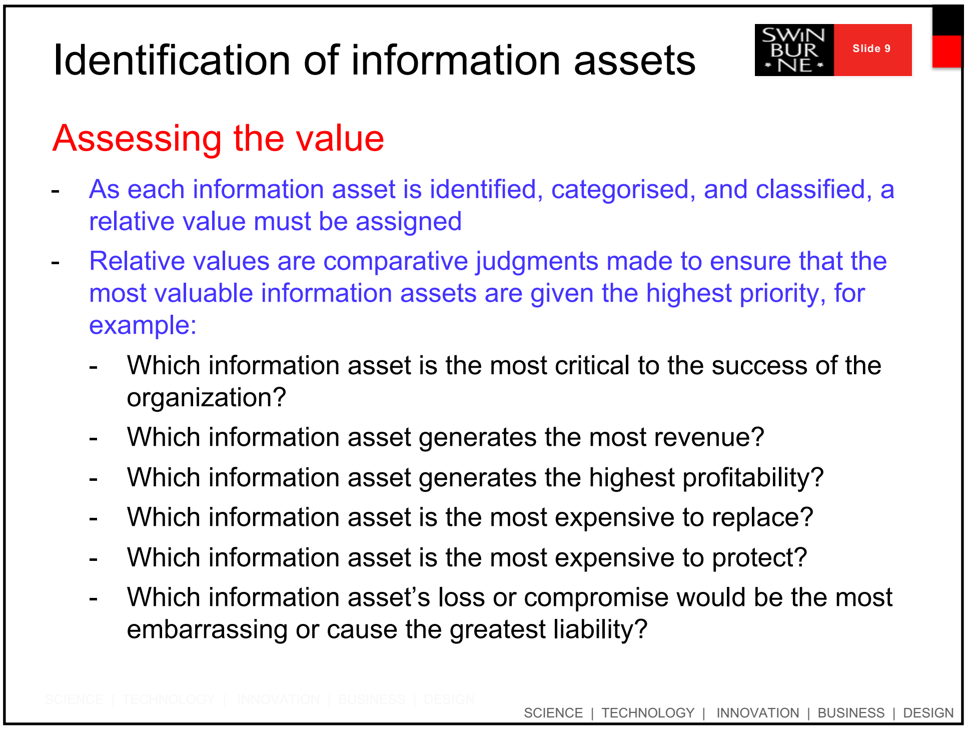
Information System Components	Risk Management Components	Example Risk Management Components
People	Internal personnel External personnel	Trusted employees Other staff members People we trust outside our organization Strangers
Procedures	Procedures	IT and business-standard procedures IT and business-sensitive procedures
* Data	Data/information Records	Transmission Processing Storage
Software	Software	Applications Operating systems Utilities Security components
Hardware	Hardware	Systems and peripherals Security devices Network-attached process control devices and other embedded systems (Internet of Things)
Networking	Networking	Local area network components Intranet components Internet or extranet components Cloud-based components

Records: *something recorded to provide evidence of something else*

Information serving a business purpose

A digital asset

8



Identification of information assets

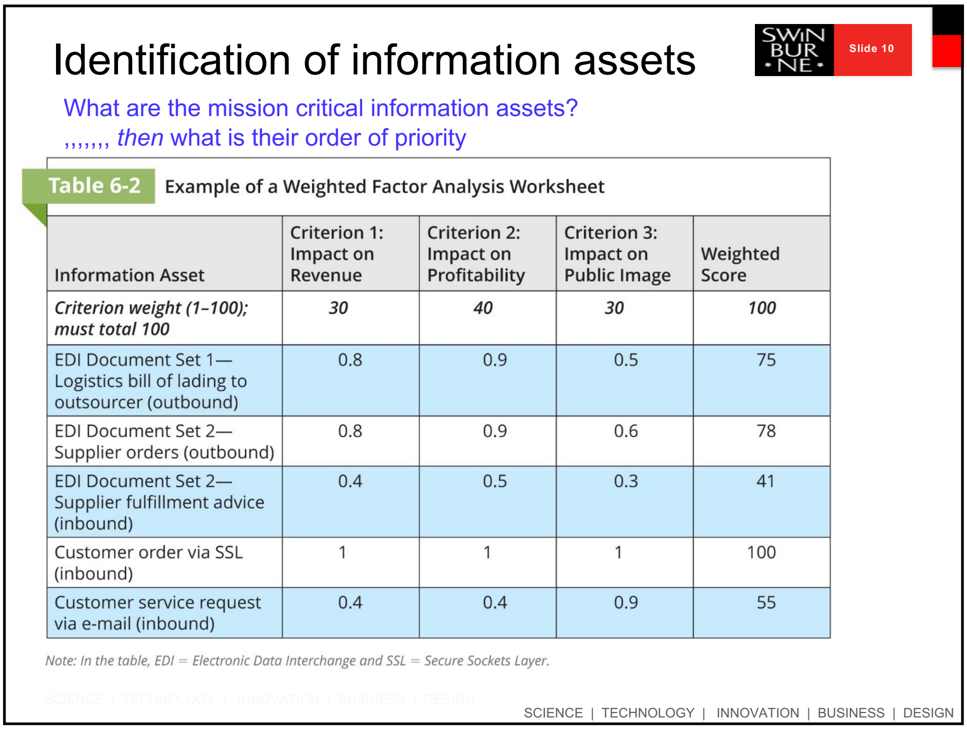
Slide 9

Assessing the value

- As each information asset is identified, categorised, and classified, a relative value must be assigned
- Relative values are comparative judgments made to ensure that the most valuable information assets are given the highest priority, for example:
  - Which information asset is the most critical to the success of the organization?
  - Which information asset generates the most revenue?
  - Which information asset generates the highest profitability?
  - Which information asset is the most expensive to replace?
  - Which information asset is the most expensive to protect?
  - Which information asset's loss or compromise would be the most embarrassing or cause the greatest liability?

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

9



Identification of information assets

Slide 10

What are the mission critical information assets?
,,,,,,, *then* what is their order of priority

Table 6-2 Example of a Weighted Factor Analysis Worksheet

Information Asset	Criterion 1: Impact on Revenue	Criterion 2: Impact on Profitability	Criterion 3: Impact on Public Image	Weighted Score
Criterion weight (1–100); must total 100	*30*	*40*	*30*	*100*
EDI Document Set 1—Logistics bill of lading to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1	1	1	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

Note: In the table, EDI = Electronic Data Interchange and SSL = Secure Sockets Layer.

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

10

Identification of information assets

Assessing risks

- Armed with a properly classified inventory, you can assess potential *weaknesses* in each information asset in relation to likely threats —a process known as threat assessment

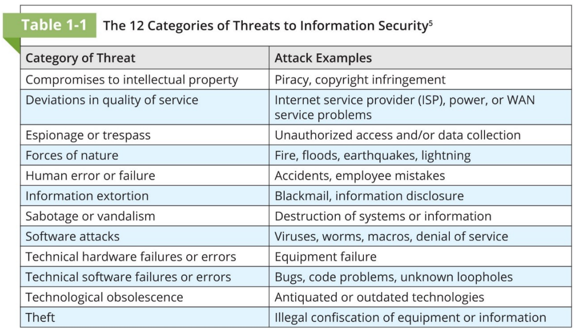


Table 1-1 The 12 Categories of Threats to Information Security[5]

Category of Threat	Attack Examples
Compromises to intellectual property	Piracy, copyright infringement
Deviations in quality of service	Internet service provider (ISP), power, or WAN service problems
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, floods, earthquakes, lightning
Human error or failure	Accidents, employee mistakes
Information extortion	Blackmail, information disclosure
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

Any organisation typically faces a wide variety of threats; if you assume that every threat can and will attack every information asset, then the project scope becomes too complex

Thus, why we focus on assessing likelihood and impact

Information Security

What is information security?

Information security (InfoSec) *the protection of information and the characteristics that give it value*, (such as **confidentiality**, **integrity**, and **availability).**

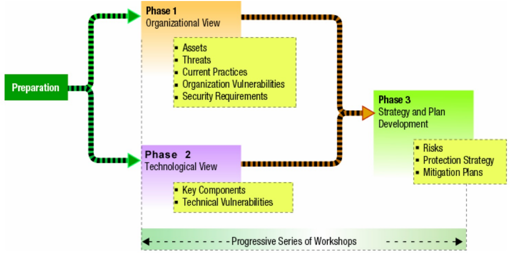
It includes the ICT that houses and transfers that information through a variety of protections such as **policy**, **procedure, process**, **training & awareness**, and **technology** (controls)

Whitman & Matford, Chapter 1

Information Security

Slide 13

Information Systems Risk Assessment methodologies



Preparation

Phase 1
Organizational View
- Assets
- Threats
- Current Practices
- Organization Vulnerabilities
- Security Requirements

Phase 2
Technological View
- Key Components
- Technical Vulnerabilities

Phase 3
Strategy and Plan Development
- Risks
- Protection Strategy
- Mitigation Plans

Progressive Series of Workshops

An organization makes information protection decisions based on operational risks and security practices

OCTAVE is a risk- based strategic assessment and planning technique for security. (*The Operationally Critical Threat, Asset, and Vulnerability Evaluation)*

"Focus on protecting key information assets"

US DoD and Carnegie Mellon, EU agencies , UK agencies

1. Identify assets and what is being done to protect those assets
2. Identify the critical assets and what is required to protect them
3. Identify vulnerabilities to critical assets
4. Identify threats to critical assets (and what is required to protect them from harm - *safeguarding*)

13

Information Security

Slide 14

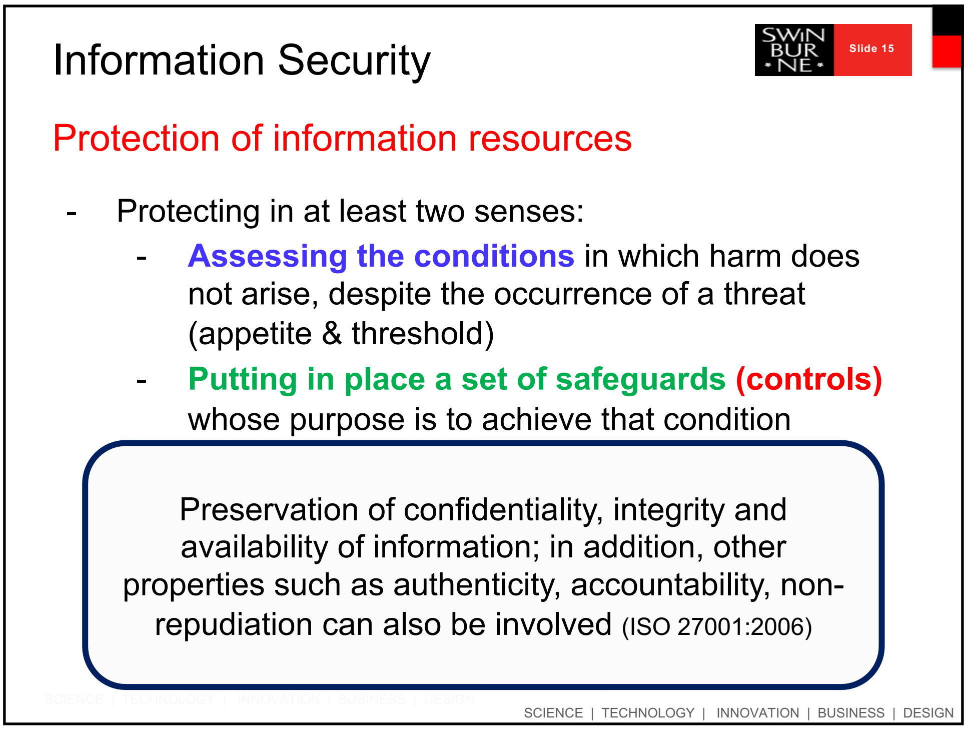
What is information security? An asset view

"*Security is a state of being free from doubt or danger.* ***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)

14

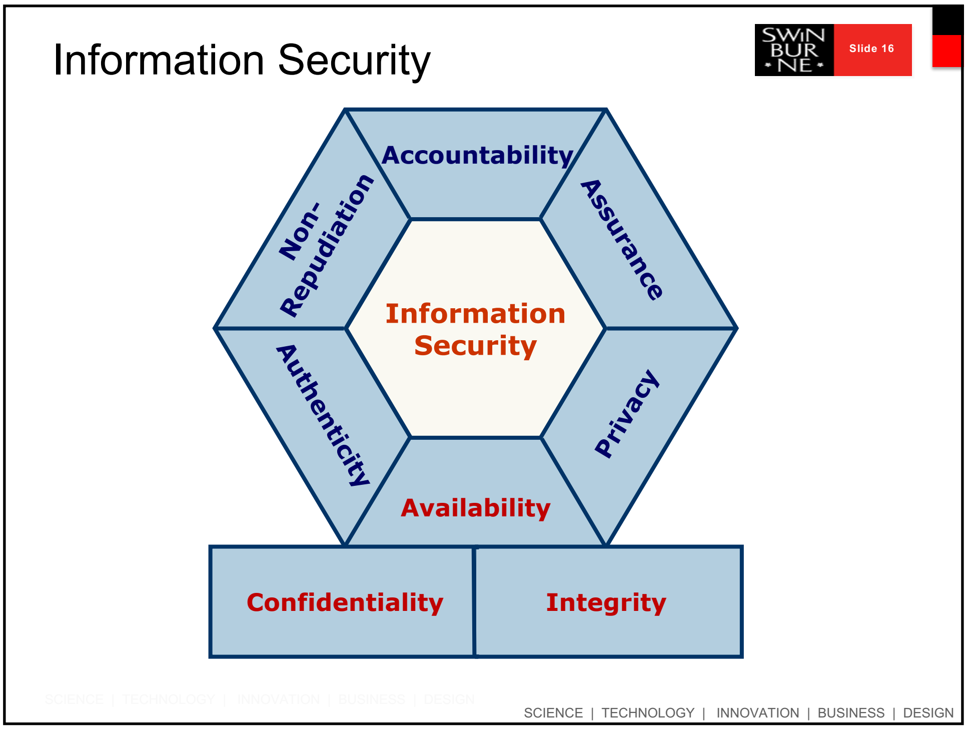


Information Security

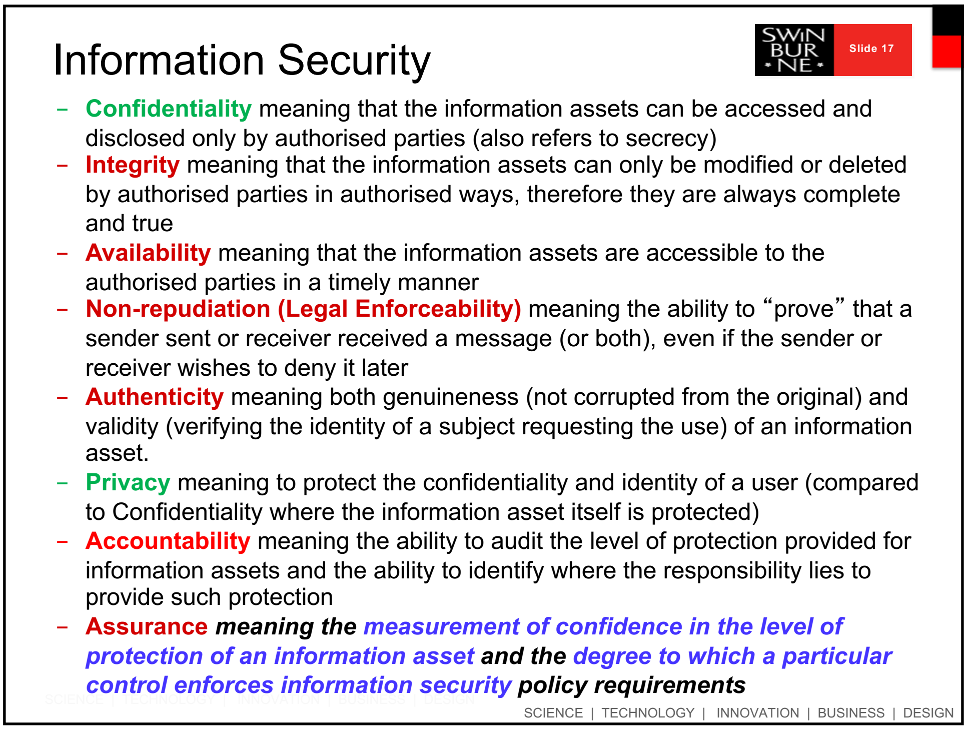
Protection of information resources

- Protecting in at least two senses:
  - **Assessing the conditions** in which harm does not arise, despite the occurrence of a threat (appetite & threshold)
  - **Putting in place a set of safeguards (controls)** whose purpose is to achieve that condition

> 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)



Information Security



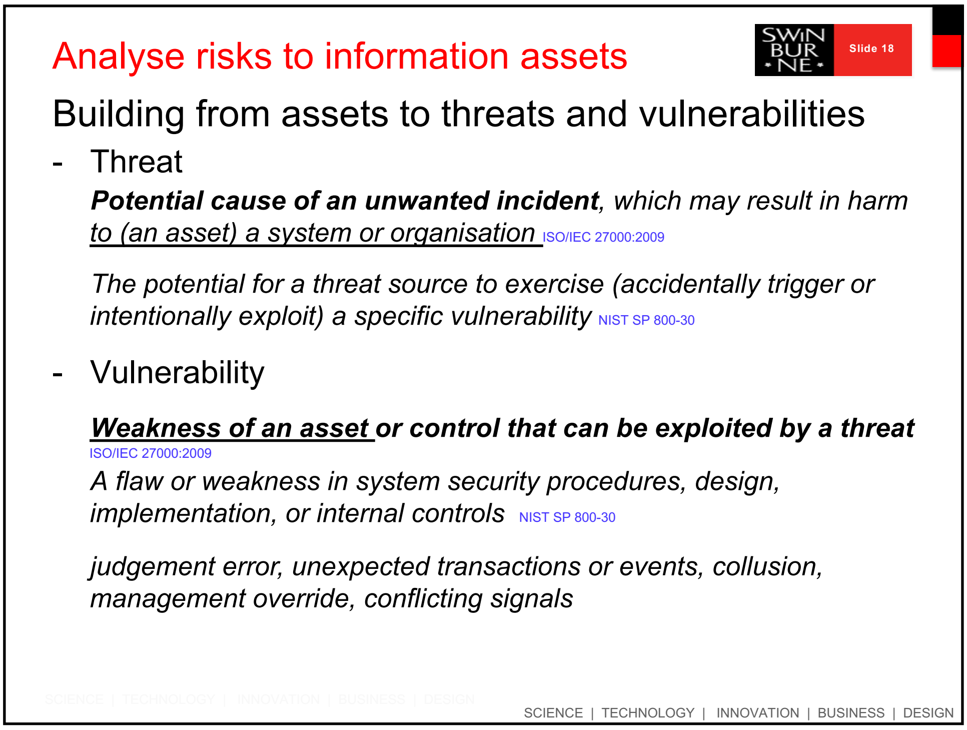
Information Security

Slide 17

- **Confidentiality** meaning that the information assets can be accessed and disclosed only by authorised parties (also refers to secrecy)
- **Integrity** meaning that the information assets can only be modified or deleted by authorised parties in authorised ways, therefore they are always complete and true
- **Availability** meaning that the information assets are accessible to the authorised parties in a timely manner
- **Non-repudiation (Legal Enforceability)** meaning the ability to “prove” that a sender sent or receiver received a message (or both), even if the sender or receiver wishes to deny it later
- **Authenticity** meaning both genuineness (not corrupted from the original) and validity (verifying the identity of a subject requesting the use) of an information asset.
- **Privacy** meaning to protect the confidentiality and identity of a user (compared to Confidentiality where the information asset itself is protected)
- **Accountability** meaning the ability to audit the level of protection provided for information assets and the ability to identify where the responsibility lies to provide such protection
- **Assurance** ***meaning the measurement of confidence in the level of protection of an information asset and the degree to which a particular control enforces information security policy requirements***

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

17



Analyse risks to information assets

Slide 18

Building from assets to threats and vulnerabilities

- Threat

  Potential cause of an unwanted incident*, which may result in harm to (an asset) a system or organisation* ISO/IEC 27000:2009

  The potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability NIST SP 800-30

- Vulnerability

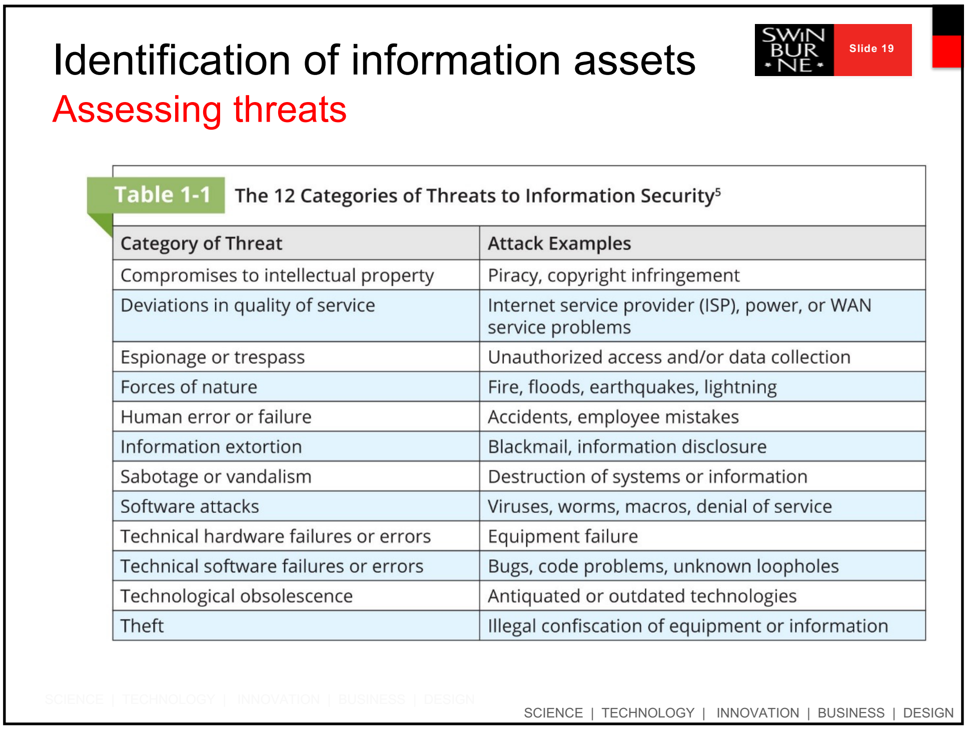
  Weakness of an asset or control that can be exploited by a threat ISO/IEC 27000:2009

  A flaw or weakness in system security procedures, design, implementation, or internal controls NIST SP 800-30

  judgement error, unexpected transactions or events, collusion, management override, conflicting signals

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

18



Identification of information assets

Assessing threats

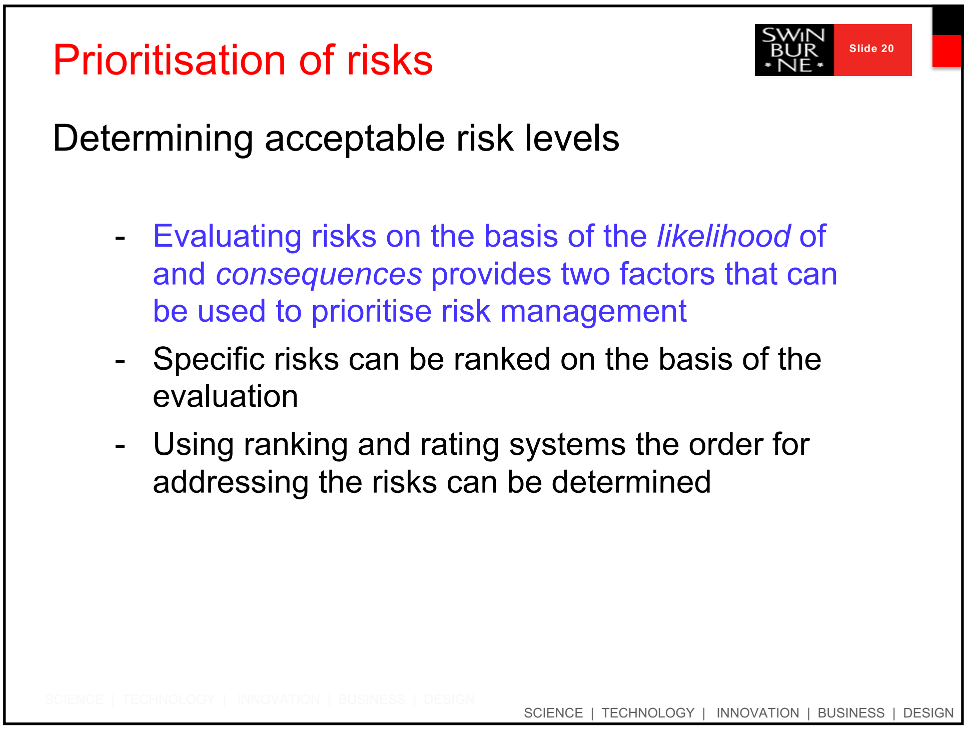
Slide 19

Table 1-1 The 12 Categories of Threats to Information Security[5]

Category of Threat	Attack Examples
Compromises to intellectual property	Piracy, copyright infringement
Deviations in quality of service	Internet service provider (ISP), power, or WAN service problems
Espionage or trespass	Unauthorized access and/or data collection
Forces of nature	Fire, floods, earthquakes, lightning
Human error or failure	Accidents, employee mistakes
Information extortion	Blackmail, information disclosure
Sabotage or vandalism	Destruction of systems or information
Software attacks	Viruses, worms, macros, denial of service
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies
Theft	Illegal confiscation of equipment or information

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

19



Prioritisation of risks

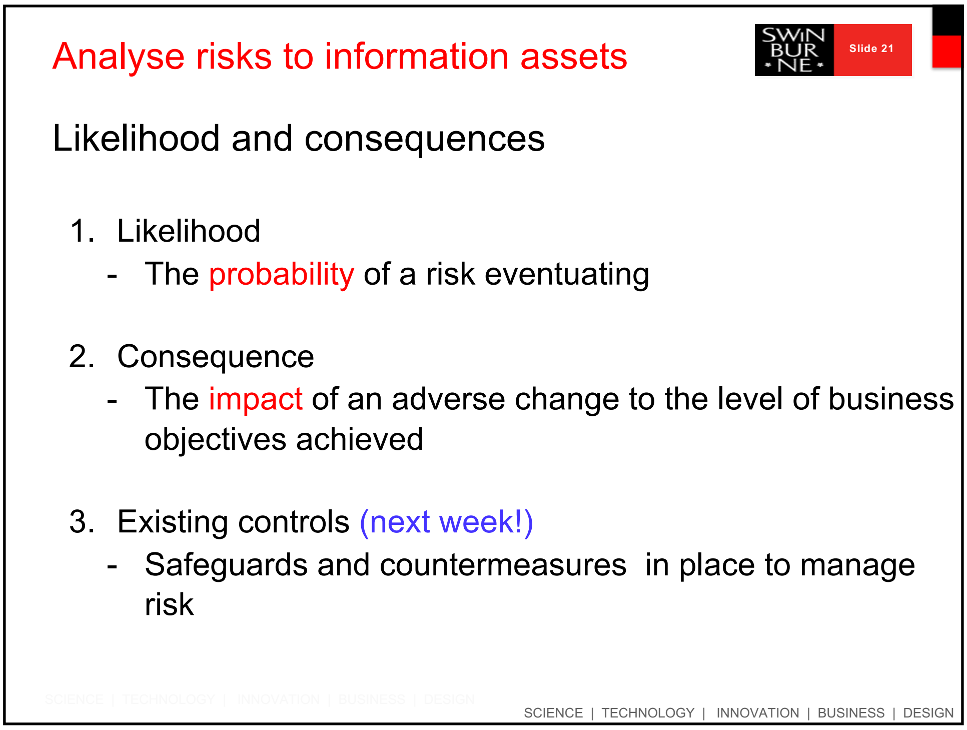
Slide 20

Determining acceptable risk levels

- Evaluating risks on the basis of the *likelihood* of and *consequences* provides two factors that can be used to prioritise risk management
- Specific risks can be ranked on the basis of the evaluation
- Using ranking and rating systems the order for addressing the risks can be determined

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

20



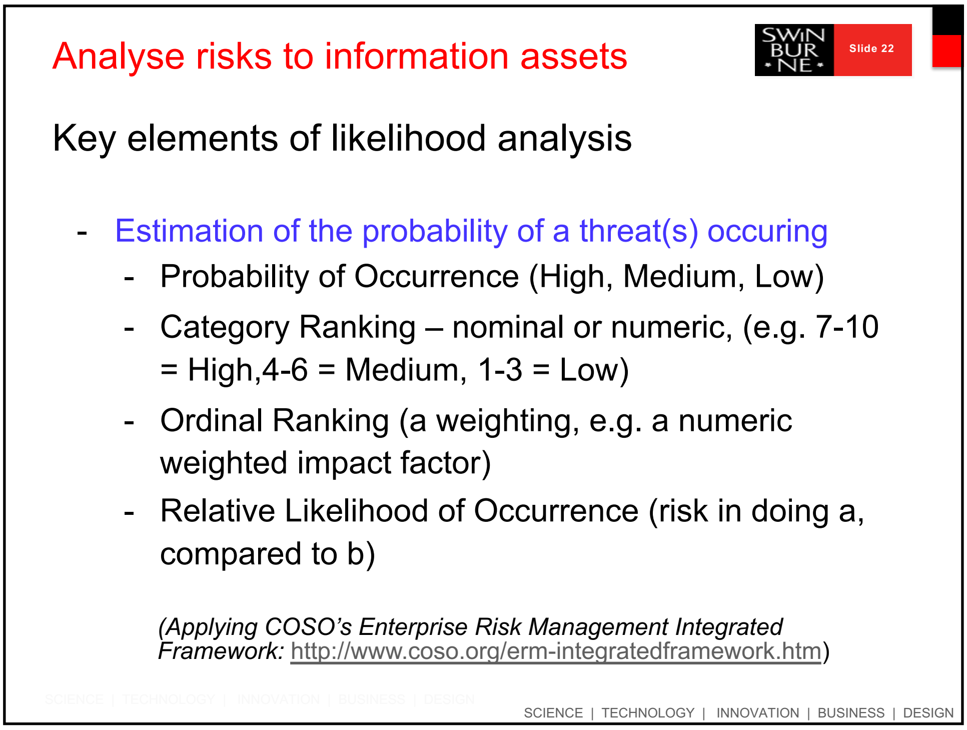
Analyse risks to information assets

Likelihood and consequences

1. Likelihood
   - The probability of a risk eventuating

2. Consequence
   - The impact of an adverse change to the level of business objectives achieved

3. Existing controls (next week!)
   - Safeguards and countermeasures in place to manage risk

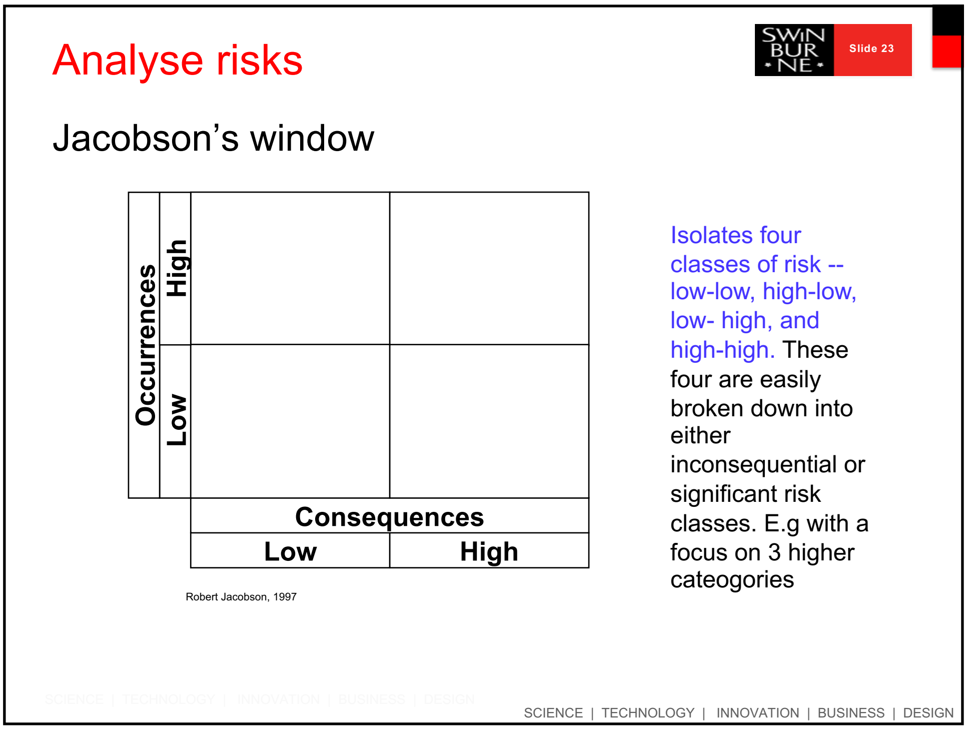


Analyse risks to information assets

Key elements of likelihood analysis

- Estimation of the probability of a threat(s) occuring
  - Probability of Occurrence (High, Medium, Low)
  - Category Ranking – nominal or numeric, (e.g. 7-10 = High,4-6 = Medium, 1-3 = Low)
  - Ordinal Ranking (a weighting, e.g. a numeric weighted impact factor)
  - Relative Likelihood of Occurrence (risk in doing a, compared to b)

(Applying COSO's Enterprise Risk Management Integrated Framework: http://www.coso.org/erm-integratedframework.htm)



Slide 23

Analyse risks

Jacobson's window

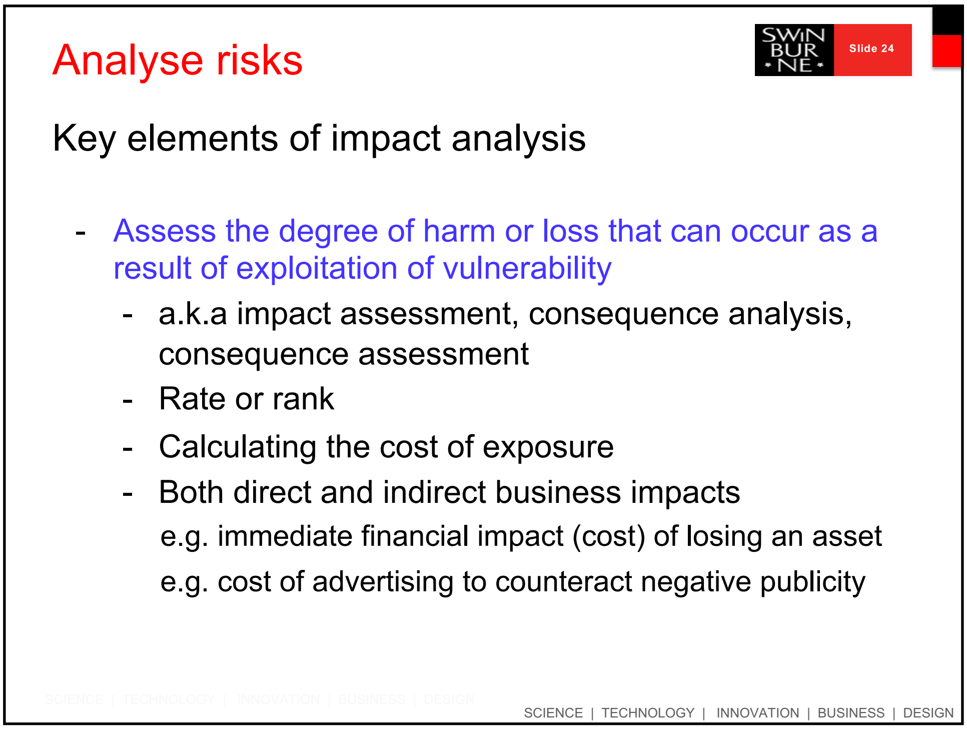
Occurrences	High		
	Low		
		Consequences	
		Low	High

Robert Jacobson, 1997

Isolates four classes of risk -- low-low, high-low, low- high, and high-high. These four are easily broken down into either inconsequential or significant risk classes. E.g with a focus on 3 higher cateogories

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

23



Slide 24

Analyse risks

Key elements of impact analysis

- Assess the degree of harm or loss that can occur as a result of exploitation of vulnerability
  - a.k.a impact assessment, consequence analysis, consequence assessment
  - Rate or rank
  - Calculating the cost of exposure
  - Both direct and indirect business impacts

    e.g. immediate financial impact (cost) of losing an asset

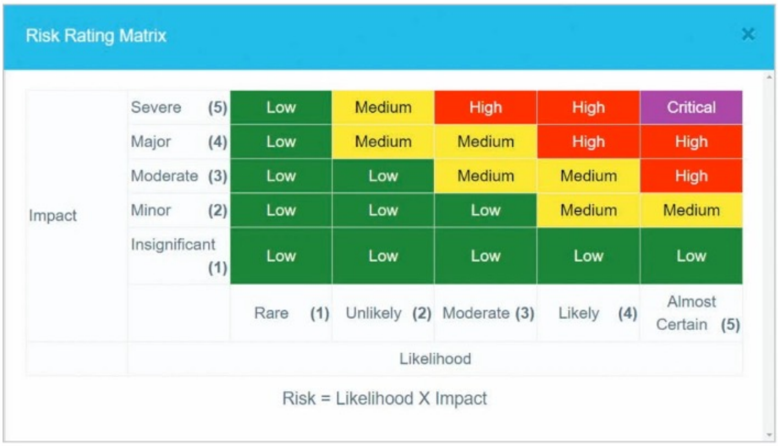
    e.g. cost of advertising to counteract negative publicity

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

24

Determining acceptable risk levels

SWIN BUR NE Slide 25



Risk Rating Matrix

Impact						
	Severe (5)	Low	Medium	High	High	Critical
	Major (4)	Low	Medium	Medium	High	High
	Moderate (3)	Low	Low	Medium	Medium	High
	Minor (2)	Low	Low	Low	Medium	Medium
	Insignificant (1)	Low	Low	Low	Low	Low
		Rare (1)	Unlikely (2)	Moderate (3)	Likely (4)	Almost Certain (5)
		Likelihood				

Risk = Likelihood X Impact

Figure 6-10 Clearwater Compliance IRM risk rating matrix

Source: Clearwater Compliance IRM.

Whitman, Michael E. and Mattord, Herbert J. *Management of information security*. Sixth Edition., Stamford, Conn. : Cengage Learning, Chapter 6

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

25

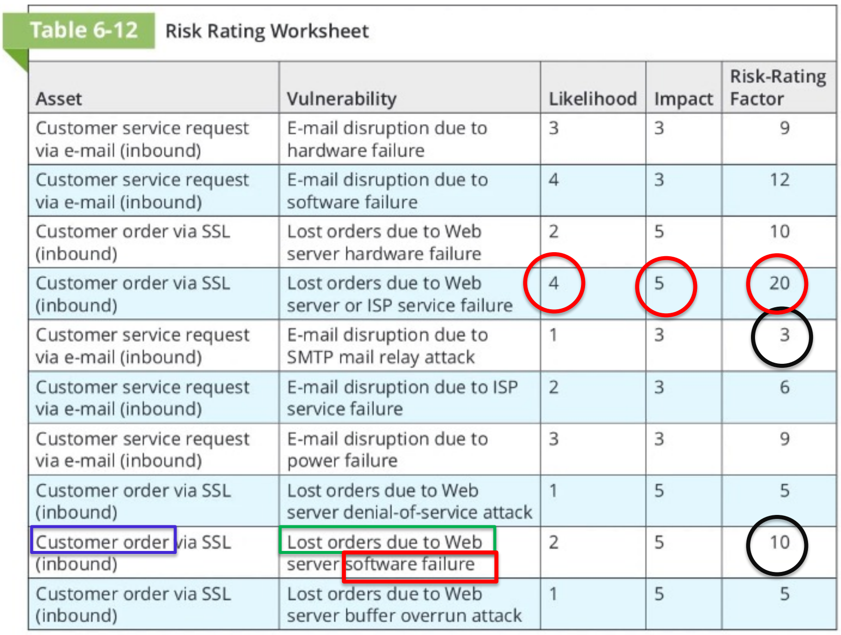
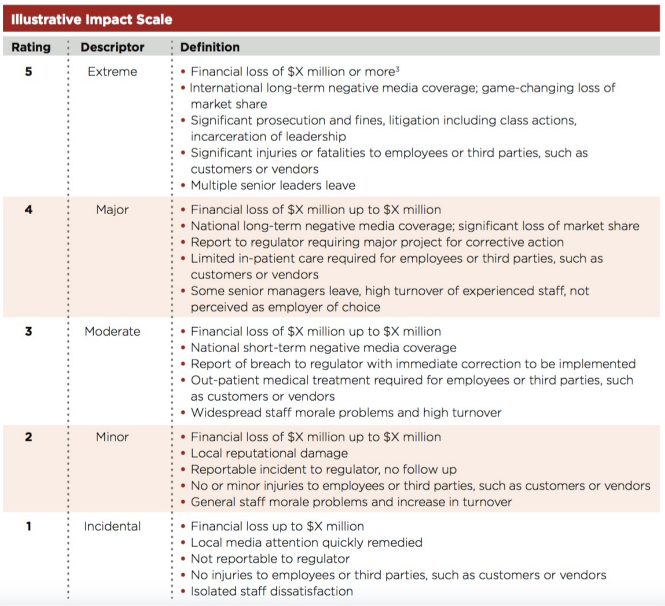


Table 6-12 Risk Rating Worksheet

Asset	Vulnerability	Likelihood	Impact	Risk-Rating Factor
Customer service request via e-mail (inbound)	E-mail disruption due to hardware failure	3	3	9
Customer service request via e-mail (inbound)	E-mail disruption due to software failure	4	3	12
Customer order via SSL (inbound)	Lost orders due to Web server hardware failure	2	5	10
Customer order via SSL (inbound)	Lost orders due to Web server or ISP service failure	4	5	20
Customer service request via e-mail (inbound)	E-mail disruption due to SMTP mail relay attack	1	3	3
Customer service request via e-mail (inbound)	E-mail disruption due to ISP service failure	2	3	6
Customer service request via e-mail (inbound)	E-mail disruption due to power failure	3	3	9
Customer order via SSL (inbound)	Lost orders due to Web server denial-of-service attack	1	5	5
Customer order via SSL (inbound)	Lost orders due to Web server software failure	2	5	10
Customer order via SSL (inbound)	Lost orders due to Web server buffer overrun attack	1	5	5

26

COSO: Risk assessment in practice

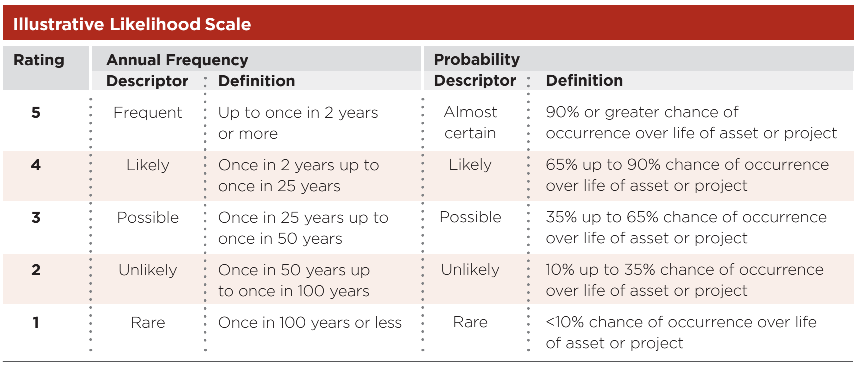


Illustrative Impact Scale

Rating	Descriptor	Definition
5	Extreme	• Financial loss of $X million or more[3] • International long-term negative media coverage; game-changing loss of market share • Significant prosecution and fines, litigation including class actions, incarceration of leadership • Significant injuries or fatalities to employees or third parties, such as customers or vendors • Multiple senior leaders leave
4	Major	• Financial loss of $X million up to $X million • National long-term negative media coverage; significant loss of market share • Report to regulator requiring major project for corrective action • Limited in-patient care required for employees or third parties, such as customers or vendors • Some senior managers leave, high turnover of experienced staff, not perceived as employer of choice
3	Moderate	• Financial loss of $X million up to $X million • National short-term negative media coverage • Report of breach to regulator with immediate correction to be implemented • Out-patient medical treatment required for employees or third parties, such as customers or vendors • Widespread staff morale problems and high turnover
2	Minor	• Financial loss of $X million up to $X million • Local reputational damage • Reportable incident to regulator, no follow up • No or minor injuries to employees or third parties, such as customers or vendors • General staff morale problems and increase in turnover
1	Incidental	• Financial loss up to $X million • Local media attention quickly remedied • Not reportable to regulator • No injuries to employees or third parties, such as customers or vendors • Isolated staff dissatisfaction

Different ranking & rating systems for likelihood, impact and risk prioritisation

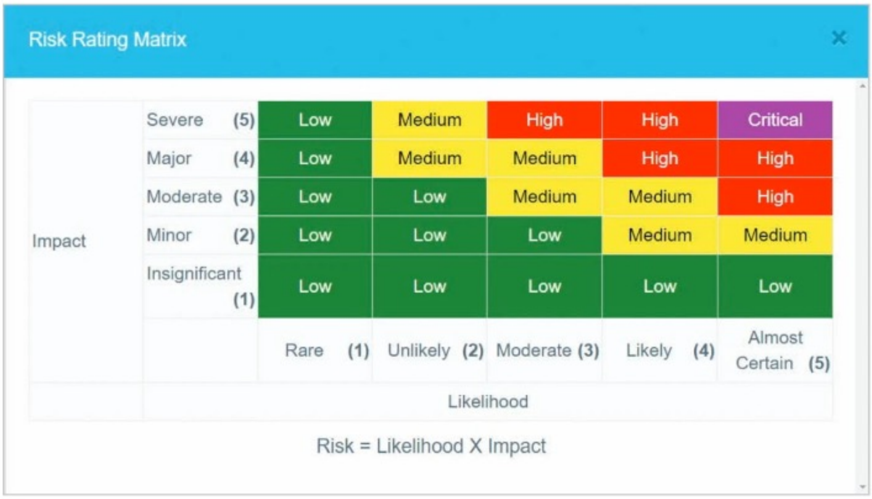
COSO: Risk assessment in practice



Illustrative Likelihood Scale

Rating	Annual Frequency		Probability	
	Descriptor	Definition	Descriptor	Definition
5	Frequent	Up to once in 2 years or more	Almost certain	90% or greater chance of occurrence over life of asset or project
4	Likely	Once in 2 years up to once in 25 years	Likely	65% up to 90% chance of occurrence over life of asset or project
3	Possible	Once in 25 years up to once in 50 years	Possible	35% up to 65% chance of occurrence over life of asset or project
2	Unlikely	Once in 50 years up to once in 100 years	Unlikely	10% up to 35% chance of occurrence over life of asset or project
1	Rare	Once in 100 years or less	Rare	<10% chance of occurrence over life of asset or project

Different ranking & rating systems for likelihood, impact and risk prioritisation



Risk Rating Matrix

Impact						
	Severe (5)	Low	Medium	High	High	Critical
	Major (4)	Low	Medium	Medium	High	High
	Moderate (3)	Low	Low	Medium	Medium	High
	Minor (2)	Low	Low	Low	Medium	Medium
	Insignificant (1)	Low	Low	Low	Low	Low
		Rare (1)	Unlikely (2)	Moderate (3)	Likely (4)	Almost Certain (5)
		Likelihood				

Risk = Likelihood X Impact

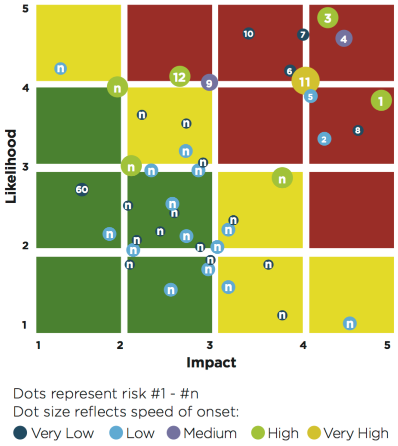
Figure 6-10 Clearwater Compliance IRM risk rating matrix

Source: Clearwater Compliance IRM.

Whitman, Chapter 6

COSO: Risk assessment in practice

Exhibit 7: Illustrative Heat Map



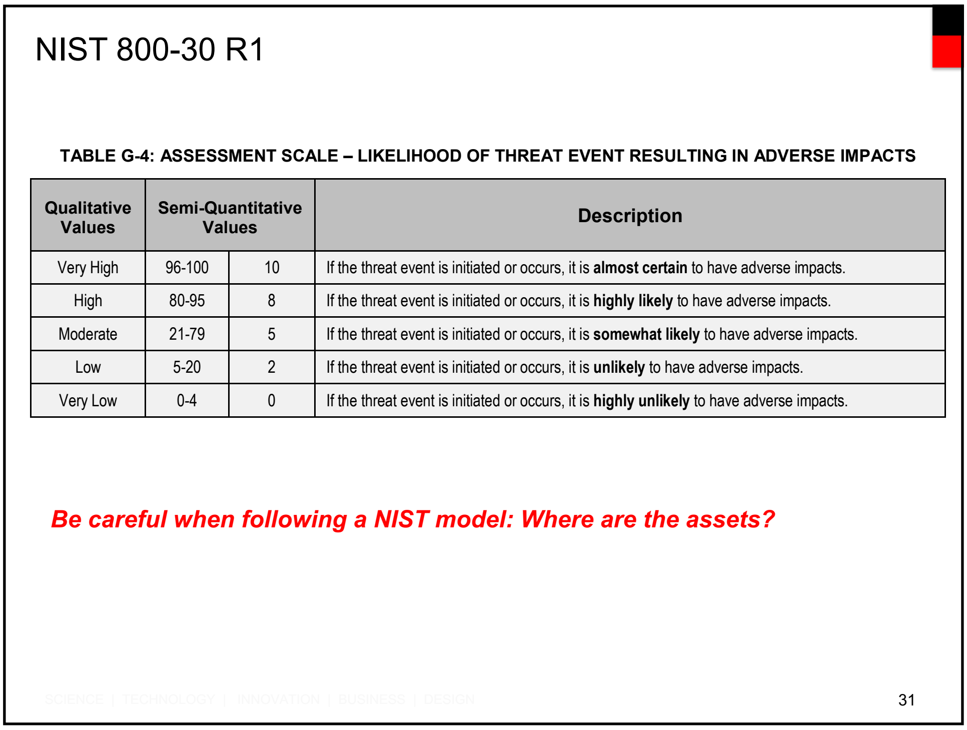
Dots represent risk #1 - #n

Dot size reflects speed of onset:

● Very Low ● Low ● Medium ● High ● Very High

ID	Risk	I	L	V	S
1	Supply chain disruption	4.8	3.7	3.8	4
2	Customer preference shift	4.1	3.3	3.5	2
3	Copper price rise >10%	4.3	4.7	2.3	4
4	Work stoppage > 1 week	4.4	4.5	4.1	3
5	Economic downturn	4.0	3.7	3.5	2
6	Supplier consolidation	3.8	4.2	3.2	1
7	Local competitors enter	3.9	4.5	3.6	1
8	New substitutes available	4.5	3.6	4.2	1
9	Cost of capital rise >5%	2.9	4.0	2.9	3
10	Tighter emission standards	3.4	4.6	2.9	1
11	FCPA violation	4.0	4.0	3.3	5
12	Exchange rate fluctuations	2.7	4.1	2.7	4
n	. . .	...	...	...	...
60	Impairment of assets	1.6	2.7	1.6	1

I = Impact L = Likelihood V = Vulnerability S = Speed of onset

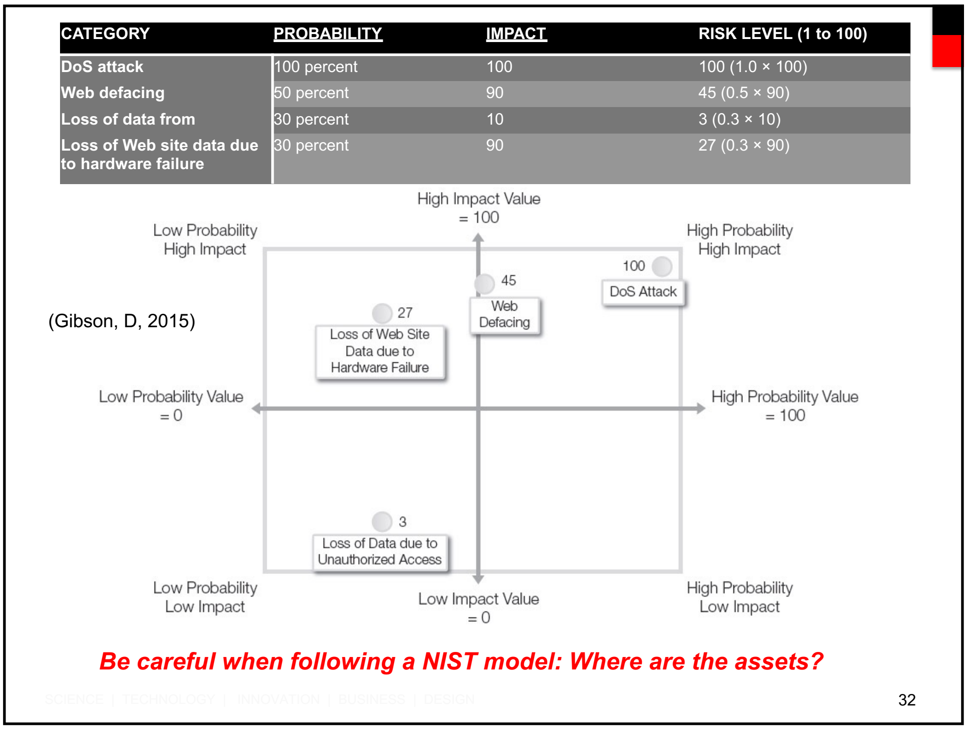


NIST 800-30 R1

TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is **almost certain** to have adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is **highly likely** to have adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is **somewhat likely** to have adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is **unlikely** to have adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is **highly unlikely** to have adverse impacts.

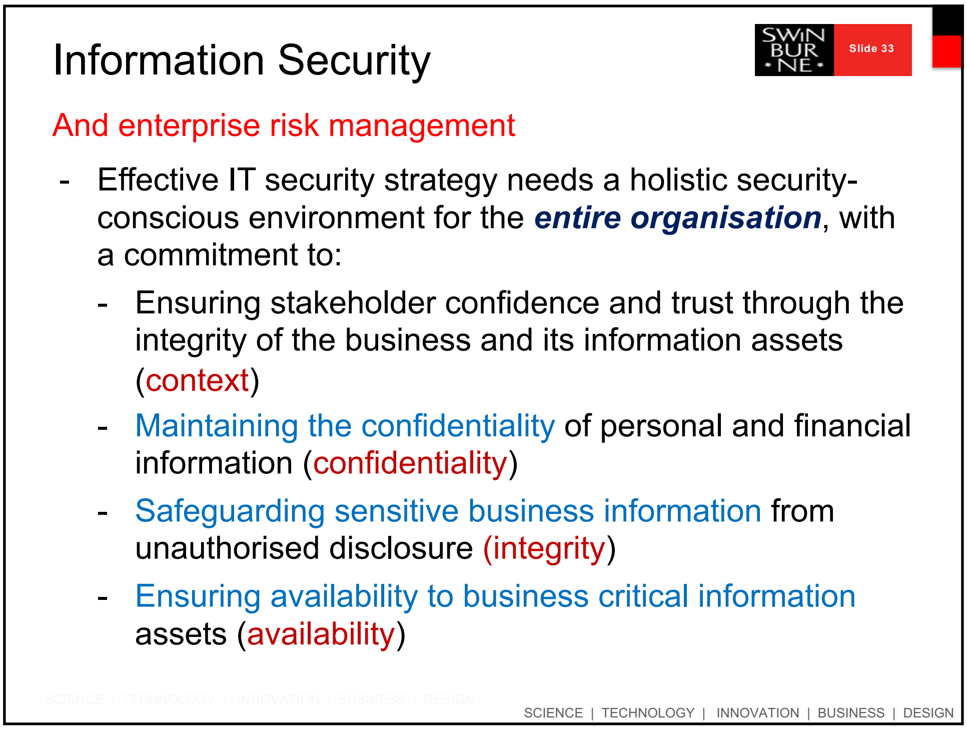
Be careful when following a NIST model: Where are the assets?



CATEGORY	PROBABILITY	IMPACT	RISK LEVEL (1 to 100)
DoS attack	100 percent	100	100 (1.0 × 100)
Web defacing	50 percent	90	45 (0.5 × 90)
Loss of data from	30 percent	10	3 (0.3 × 10)
Loss of Web site data due to hardware failure	30 percent	90	27 (0.3 × 90)

(Gibson, D, 2015)

Be careful when following a NIST model: Where are the assets?



Information Security

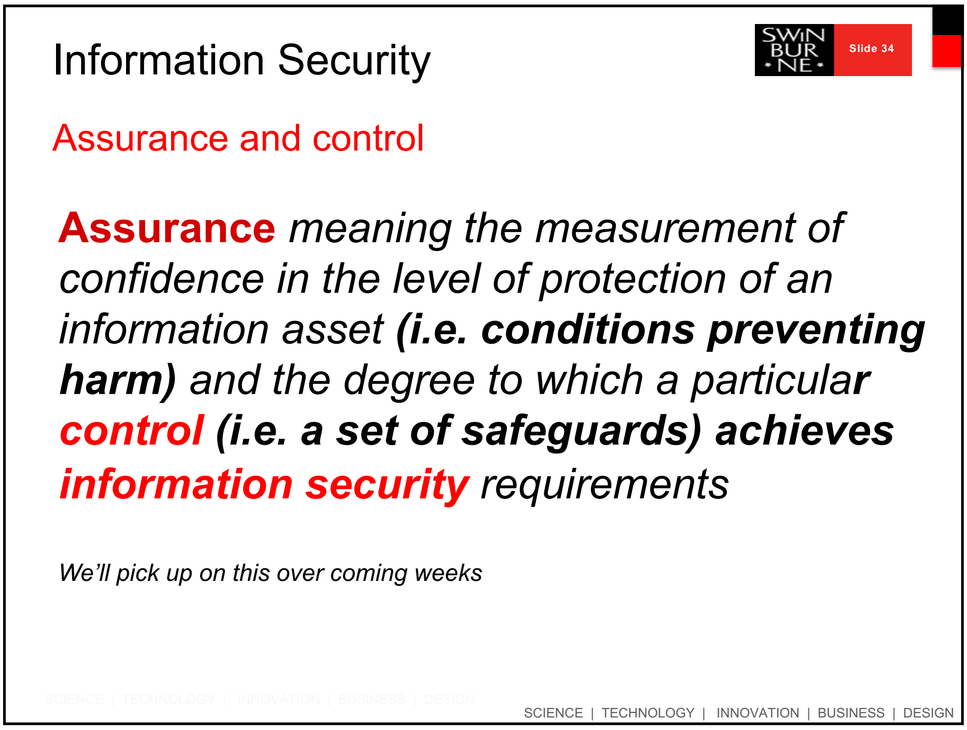
Slide 33

And enterprise risk management

- Effective IT security strategy needs a holistic security-conscious environment for the ***entire organisation***, with a commitment to:
  - Ensuring stakeholder confidence and trust through the integrity of the business and its information assets (context)
  - Maintaining the confidentiality of personal and financial information (confidentiality)
  - Safeguarding sensitive business information from unauthorised disclosure (integrity)
  - Ensuring availability to business critical information assets (availability)

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

33



Information Security

Slide 34

Assurance and control

Assurance *meaning the measurement of confidence in the level of protection of an information asset* ***(i.e. conditions preventing harm)*** *and the degree to which a particular* ***control (i.e. a set of safeguards) achieves information security*** *requirements*

We'll pick up on this over coming weeks

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

34

Terms & processes to follow up on: Risk assessment, Risk identification Identification of information assets, Prioritising assets, Analysing risks to assets

Continue with your readings and review, of Whitman, Gibson and standards

SWINBURNE UNIVERSITY OF TECHNOLOGY
Swinburne
think forward

35