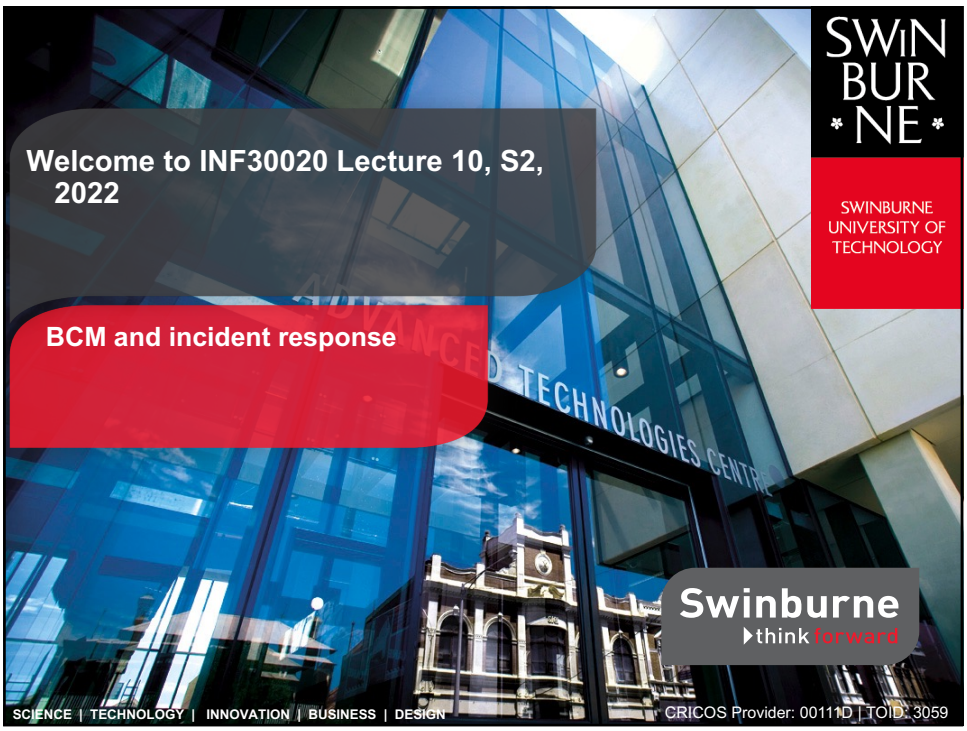


1

Summary, schedule and assessment

Slide 2

01 August	Introduction and Overview: IS risk and security	Class activity & reading (TBA)
08 August	Information Security & risks I	Class activity & reading (TBA); Submit CLA #1, Friday 12 August
15 August	Information Security & risks II	Class activity & reading (TBA)
22 August	Identifying Information Assets & evaluating risks	Class activity & reading (TBA); Submit CLA #2, Friday 26 August
29 August	Mitigation, treatment & control I	Class activity & reading (TBA)
05 September	Mitigation, treatment & control II	Class activity & reading (TBA); Submit Online Quiz #1, Friday 09 September
19 September	Information Security & Information Governance	Group Warm-up (TBA); Submit in class, Wednesday 21 September
26 September	Business Continuity Management	Class activity & reading (TBA);
03 October	Contingency Planning	Class activity & reading (TBA); Submit CLA #3, Friday 07 October
10 October	Cybersecurity and Business Continuity Management	Class activity & reading (TBA);
17 October	Fraud and forensic auditing: Fraud, cybercrime, forensic auditing and continuous monitoring	Class activity & reading (TBA); Submit Report Part B, Friday 21 October
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 – M009 completed

Assessments

- CLA#1 , CLA#2 submitted and returned marking, CLA#3 submitted
- Group warm up exercise completed (*those present receive mark*)
- Quiz 1 completed, Quiz 2 in week 12

Groups

- Group assignment
  - was due Friday 21 October, 11:59pm
  - Now due Tuesday 25 October, 9am

SCIENCE | TECHNOLOGY | INNOVATION | BUSINESS | DESIGN

2

Assignment 1

Slide 3

- *Highest score 96%,– congratulations! Mean15.5, lowest score 0.*
- On the higher end students demonstrated a clear understanding of the assignment objectives for information risk assessment (IS security based) and undertook all required steps well,
- Proposed a risk appetite and tolerance for eTricity, considered rating tolerance, evaluated roles and responsibilities identifying gaps likely to present a security concern
- Had worked through the case to inventory and understand the information assets (information resources and systems) at eTricity early in the analytical process and were able to describe these well
- Identified risks (in an , A,T,V logic that was ordered well) and connected to the most important information assets at eTricity. And, developed a good approach to describing the the threats and vulnerabilities associated with assets (rather than separating and breaking out into a T & V only evaluation)
- Undertook likelihood and impact analysis and described this well, including evaluation and prioritisation
- Usually with direct inclusion of tables and diagrams throughout, i.e. Had considered information design
- Had undertaken additional research, ***building on unit texts and standards as the first point of call***, additional resources added something e.g. were good solutions sensible to internal logic of assignment and not gratuitous
- May have included knowledge from other Degree areas ,e.g. cyber security, project management or 'Porters strategic models' but understood the significant differences in these curriculum and did not simply repeat or try passing off approaches from these units here
- *Advise going forward decide what information you want to work with from the individual assignments. My advice is cherry-pick, don't simply decide to go with the highest scoring assignment from Assignment 1*

3

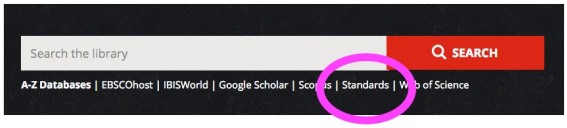
Reading for this week's topic

Unit texts:

- Whitman, Michael E. annd Mattord, Herbert J. Chapters 3, 4, 7 ,10 & 12 Planning for Contingencies. *Management of information security*. Sixth Edition., Stamford, Conn. : Cengage Learning, 2019.
- Gibson, Darril, Chapters 11-13. Chapter 11, Turning your Risk Assessment into a Risk Mitigation Plan, Chapter 12, Mitigating Risk with a Business Impact Analysis, Chapter 13, Mitigating Risk with a Business Continuity Plan, *Managing Risk in Information Systems*. 2015.

Additional reading list

- HB292-2006 – (A Practitioners Guide to Business Continuity Management , Swinburne Library SAI Database)
- Gibson Chapters 11- 15
- Whitman Chapters 7, 10, 12



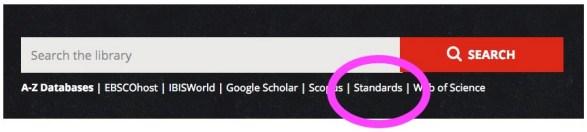
4

Business continuity management

Slide 5

BCM Standards and guidelines (ISO 22301: 2019)

- HB292-2006 – (A Practitioners Guide to Business Continuity Management , Swinburne Library Techstreet Database)
- NIST800-34 Rev.1 - Contingency Planning Guide for Federal Information Systems (available online)
- The Auditor-General ANAO Report No.6 2014–15 Performance Audit: Business Continuity Management https://www.anao.gov.au/work/performance-audit/business-continuity-management **(recommended unit reading)**
- **AS ISO 22313:2017, Societal security—Business continuity management systems—Guidance**
- **SA TS ISO 22317:2017, Societal security—Business continuity management systems—Guidelines for business impact analysis (BIA)**
- **ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements**



5

This week's learning plan

Slide 6

Gain an understanding of

- *relationship between BCM and incident response*
- *relationship between information governance & information security policy*
- the role of contingency planning in terms of cybersecurity incident management
- Understand major (Cyber) Information risk and security issues for some key topic areas : *Phishing, ransomware,*

6

Your group assignment

Slide 7

A deep dive on BCM

Identify further opportunities of work in the risk management and information security management area, prioritising business continuity and incident response associated with risks to information assets you have identified and how eTricity should address them

The assignment can be considered in two halves

Items 1 - 2

- BCM planning inclusive of Information Governance, Information Security Policy & Information Security-Risk mitigation for 10-12 priorities (avoid, share, reduce, accept)

Items 3 - 4

- Advising eTricity on the need for a business continuity through BIA (top 5 critical areas), prioritized business impact assessments, with parameters for response. Develop 2 disruption scenarios and
- A brief Incident Response Plan (IRP) – handling procidurs inclusive of communications planning as part of this

7

Item 1. Information Governance

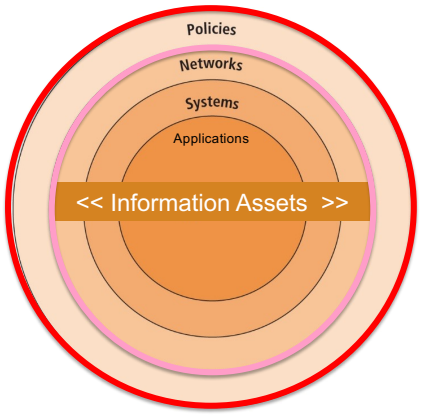
Swinburne

1. Build on Report A analyses of roles and responsibilities, including the gaps ,
2. Think about your stakeholders, roles, responsibilities, relationships (mappings)
3. Think about what eTricity guidelines (policies and procedures at major touchpoints) might need to be in place, that talks to the value of the information being protected…. e.g.
4. Is there an InfoSec policy in place anywhere? Is there and information security 'group' reporting to the Board (place infosec on the boards agenda/ instituionalised monitoring as part of control)?
5. You are not required to develop a security policy, but is it a prudent feature of IG and Internal Control to recommend the development of policy and explain
6. Think about your communications plans both for Information Governance (organisational stakeholders)
7. Crisis communication planning

See Whitman Chapter 3 & 4

8

Information Governance & Information Security policy



Enterprise information security policy is high-level information security policy that sets the strategic direction, scope, and tone for all of an organization's security efforts

An EISP is also referred to as the security program, general security policy, IT security policy, high-level InfoSec policy, or simply the InfoSec policy

See Whitman Chapter 3 & 4

9

1. State the purpose: importance of InfoSec to the organization's mission and objectives
2. Set an overview structure of the InfoSec organization and individuals who fulfill the InfoSec role
3. Provide fully articulated responsibilities for security that are shared by all members of the organization

Table 4-1 Components of the EISP

Component	Description
Purpose	Answers the question, "What is this policy for?" Provides a framework that helps the reader to understand the intent of the document. Can include text such as the following, which is taken from Washington University in St. Louis: *This document will:* • *Identify the elements of a good security policy* • *Explain the need for information security* • *Specify the various categories of information security* • *Identify the information security responsibilities and roles* • *Identify appropriate levels of security through standards and guidelines* *This document establishes an overarching security policy and direction for our company. Individual departments are expected to establish standards, guidelines, and operating procedures that adhere to and reference this policy while addressing their specific and individual needs.*[5]
Elements	Defines the whole topic of information security within the organization as well as its critical components. For example, the policy may state: "Protecting the confidentiality, integrity, and availability of information while in processing, transmission, and storage, through the use of policy, education and training, and technology" and then identify where and how the elements are used. This section can also lay out security definitions or philosophies to clarify the policy.
Need	Justifies the need for the organization to have a program for information security. This is done by providing information on the importance of InfoSec in the organization and the obligation (legal and ethical) to protect critical information, whether regarding customers, employees, or markets.
Roles and responsibilities	Defines the staffing structure designed to support InfoSec within the organization. It will likely describe the placement of the governance elements for InfoSec as well as the categories of individuals with responsibility for InfoSec (IT department, management, users) and their InfoSec responsibilities, including maintenance of this document.
References	Lists other standards that influence and are influenced by this policy document, including relevant federal and state laws and other policies.

EISP *See Whitman Chapter 3 & 4*

10

Issue specific Information Security policy (ISSP)

- An organizational policy that provides detailed, targeted guidance to instruct all members of the organization in the use of a resources
  - ✓ *e.g. fair and responsible use policies*
- Every organization's ISSPs should:
  - ✓ Address specific technology-based systems
  - ✓ Require frequent updates
  - ✓ Contain a statement on the organization's position on an issue

See Whitman Chapter 3 & 4

11

Issue specific Information Security policy (ISSP)

- Use of electronic mail, IM, and other communications apps
- Use of the Internet, the Web, and company networks by company equipment
- Malware protection requirements
- Use of non organisationally issued software or hardware on organization assets
- Use of organisational information on non organisationally owned computers
- Prohibitions against hacking or testing security controls or attempting to modify or escalate privileges
- Personal and/or home use of company equipment

Removal of organizational equipment from organizational property

Use of personal equipment on company networks (BYOD)

Use of personal technology during work hours

Use of photocopying and scanning equipment

Requirements for storage and access to company information while outside company facilities

Specifications for the methods, scheduling, conduct, and testing of data backups

Requirements for the collection, use, protection and destruction of information assets

Storage of access control credentials by users

See Whitman Chapter 3 & 4

12

ISSP

Table 4-4 ISSP Document Organization Approaches

Approach	Advantages	Disadvantages
Individual Policy	• Clear assignment to a responsible department • Written by those with superior subject matter expertise for technology-specific systems	• Typically yields a scattershot result that fails to cover all of the necessary issues • Can suffer from poor policy dissemination, enforcement, and review
Comprehensive Policy	• Well controlled by centrally managed procedures assuring complete topic coverage • Often provides better formal procedures than when policies are individually formulated • Usually identifies processes for dissemination, enforcement, and review	• May overgeneralize the issues and skip over vulnerabilities • May be written by those with less complete subject matter expertise
Modular Policy	• Often considered an optimal balance between the individual ISSP and the comprehensive ISSP approaches • Well controlled by centrally managed procedures, assuring complete topic coverage • Clear assignment to a responsible department • Written by those with superior subject matter expertise for technology-specific systems	• May be more expensive than other alternatives • Implementation can be difficult to manage ***See Whitman Chapter 3 & 4***

13

Item 2, Risk response: selecting the best treatment option on the basis of severity and significance

Likelihood	Consequences				
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Almost certain	Accept/Control	Control	Avoid or Transfer	Avoid or Transfer	Avoid or Transfer
Likely	Accept/Control	Control	Avoid or Transfer	Avoid or Transfer	Avoid or Transfer
Possible	Accept/Control	Control	Transfer or Control	Avoid or Transfer	Avoid or Transfer
Unlikely	Accept/Control	Control	Transfer or Control	Transfer	Transfer
Rare	Accept/Control	Control	Transfer or Control	Transfer	Transfer

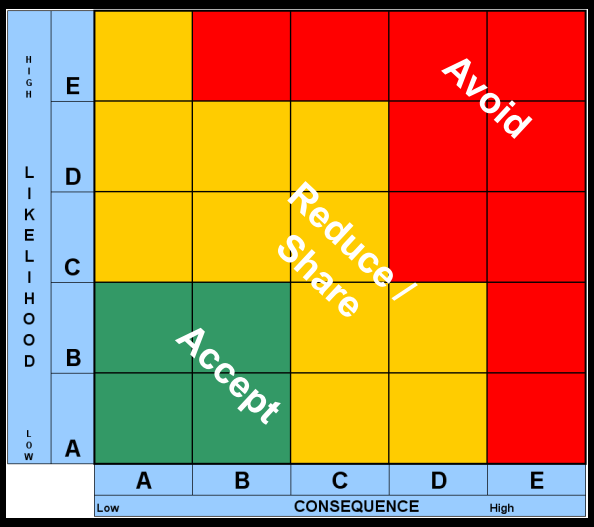
May need to simplify asset evaluations and communicate a strong mitigation strategy

14

Item 2. Risk treatment: risk response strategies

Inherent risk: The risk that an activity would pose if no controls or other mitigating factors were in place

Residual risk: The risk that remains after controls or other mitigating circumstances are taken into account



Senior Management Attention

Local Management Attention

No Action

15

Item 2. Risk treatment: risk response strategies

Control activities are
the policies, procedures, techniques, and mechanisms that are applied to help ensure that the risks identified during risk assessment are managed

1. There are hundreds of controls that can be implemented
2. When evaluating controls, best to consider different categories of control (e.g. administrative, technical, physical: prevention, detection & correction).

Gibson Chapter 9 is a great starting point for different ways of thinking about Controls , Whitman Chapter 8

16

Table 8-5 NIST Security Control Classes, Families, and Identifiers[12]

Identifier	Family	Class
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Security Assessment and Authorization	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Security	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communication Protection	Technical
SI	System and Information Integrity	Operational
PM	Program Management	Management

Source: NIST 800-53, Rev. 4.

Whitman Chapter 8, Chapter 12

17

Categories of access controls – extending PDC

Swinburne

Directive—Employs administrative controls such as policy and training designed to proscribe certain user behavior in the organization

Deterrent—Discourages or deters an incipient incident

Preventative—Helps an organization avoid an incident

Detective—Detects or identifies an incident or a threat when it occurs

Corrective—Remedies a circumstance or mitigates damage done during an incident

Recovery—Restores operating conditions back to normal

Compensating—Resolves shortcomings

Whitman Chapter 8, Chapter 12

18

Why not call this Unit *Cybersecurity?*

Slide 19

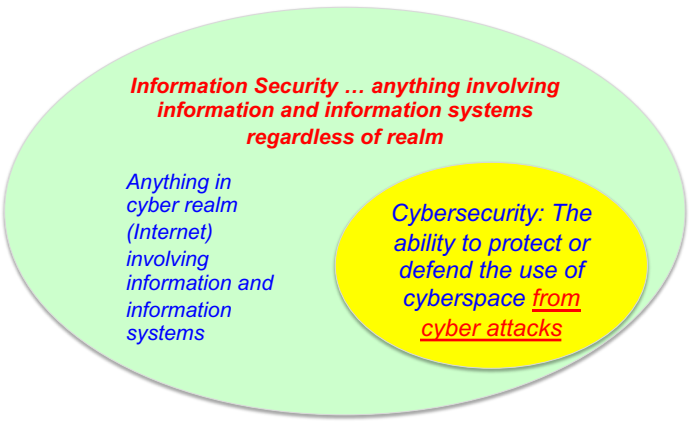
Information security involves protection of information assets (whether in digital, physical or human form) and information systems from damage, misuse or attack (whether in storage, processing, or transit), resulting in information being stable, reliable, and free of failure.

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)

Australians are increasingly connected, online and engaged

19

Slide 20



Cybersecurity:
Extends to Operational technology & to individual personal e-safety

Operational Technology (OT) – the hardware and software dedicated to direct monitoring and/or control of physical devices such as valves, pumps, etc.

https://www.novainfosec.com/2014/05/05/cyber-security-versus-information-security/

20

Framing Cyber in Information Security

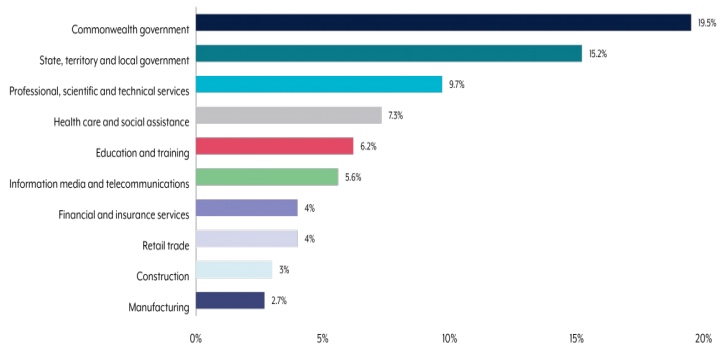
Slide 21

ISACA definition

- Cybersecurity refers to protecting information assets by addressing threats to information processed, stored and transported by information systems that are internetworked (Internet – networked)
- The threats to information assets range from basic malware, such a viruses and worms, to targeted, state-sponsored attacks, and persistent threats
  - 2015, BOM (China) , RBA http://www.abc.net.au/news/2015-12-02/cyber-attack-on-reserve-bank-computers-blamed-on-indonesia/6995532,... Australian Signals Directorate had in 2009 attempted to monitor the mobile phone calls of Indonesian President Susilo Bambang Yudhoyono,)
- Identity theft; Internet banking fraud; Phishing attacks; Shopping and auction site fraud; Online recruitment of mules, Scams (Nigerian lottery, inheritance), Ransom ware
- Enterprises of all sizes and individuals need to not only be aware of these threats, but also the processes of managing the risk involved.

21

Cyber security incidents by the top ten reporting sectors for financial year 2020–21



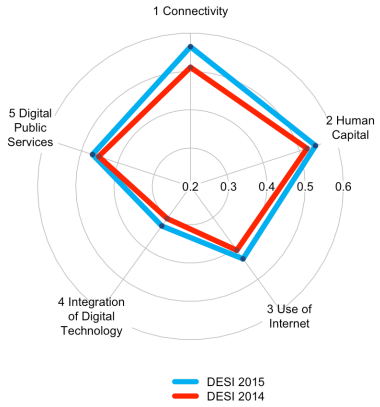
On 19 June 2020, the Prime Minister of Australia publicly announced the Australian Government is aware of and alert to the threat of cyber-attacks. The ACSC identified this threat as a Category 1 cyber incident, as it involved the sustained targeting of Australian governments and companies by a sophisticated state-based actor.

22

There are some game changers

Slide 23

- Connectivity always on, work systems accessed at home, wi-fi hotspots growing,
- Increases window and opportunity for attack
- IT Centric Business & society, online systems are the new critical infrastrcuture, often no (paper) fallback,
- Increases number of *business processes* that can be targeted
- Newer classes of systems, mobile devices remain a mystery to many, digital natives often do not have deep IT skills, *New IT (apps & operating systems) favor convenience over control,*
- Increases chance/role of human error in creation of cyber threats and vulnerabilities



EU Digital Economy & Society Index:
http://ec.europa.eu/digital-agenda/en/desi

23

Phishing: masquerading as a trusted entity

Westpac
Australia's First Bank

Dear Valued Customer,

- Our new security system will help you to avoid frequently fraud transactions and to ke investments in safety.

- Due to technical update we recommend you to reactivate your account.

Click on the link below to login and begin using your updated Westpac account.

To log into your account, please visit the NetBank website at https://olb.westpac.com.au/

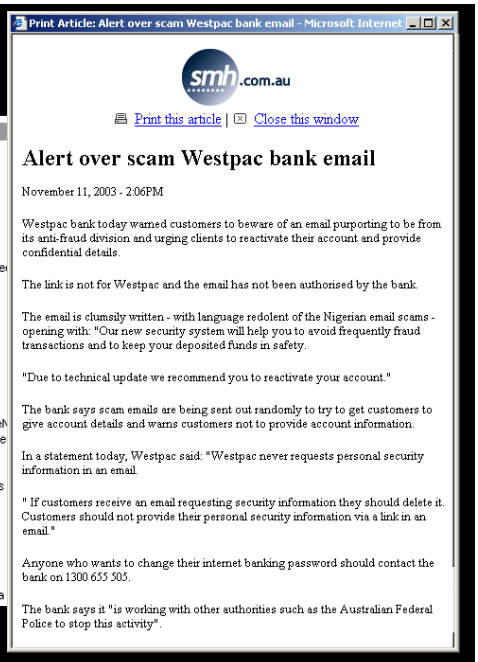
To review your statement, log into your Westpac account and click the eStatements & eN in the left navigation of your Account Summary page. Your new statement is listed in the the page.

If you have questions about your online statement, please send us a Bank Mail or call us 1-888-BKONWEB (256-6932).

We appreciate your business. It's truly our pleasure to serve you.

Westpac Customer Care

This email is for notification only. To contact us, please log into your account and send a


Print Article: Alert over scam Westpac bank email - Microsoft Internet

smh.com.au

Print this article | Close this window

Alert over scam Westpac bank email

November 11, 2003 - 2:06PM

Westpac bank today warned customers to beware of an email purporting to be from its anti-fraud division and urging clients to reactivate their account and provide confidential details.

The link is not for Westpac and the email has not been authorised by the bank.

The email is clumsily written - with language redolent of the Nigerian email scams - opening with: "Our new security system will help you to avoid frequently fraud transactions and to keep your deposited funds in safety.

"Due to technical update we recommend you to reactivate your account."

The bank says scam emails are being sent out randomly to try to get customers to give account details and warns customers not to provide account information.

In a statement today, Westpac said: "Westpac never requests personal security information in an email.

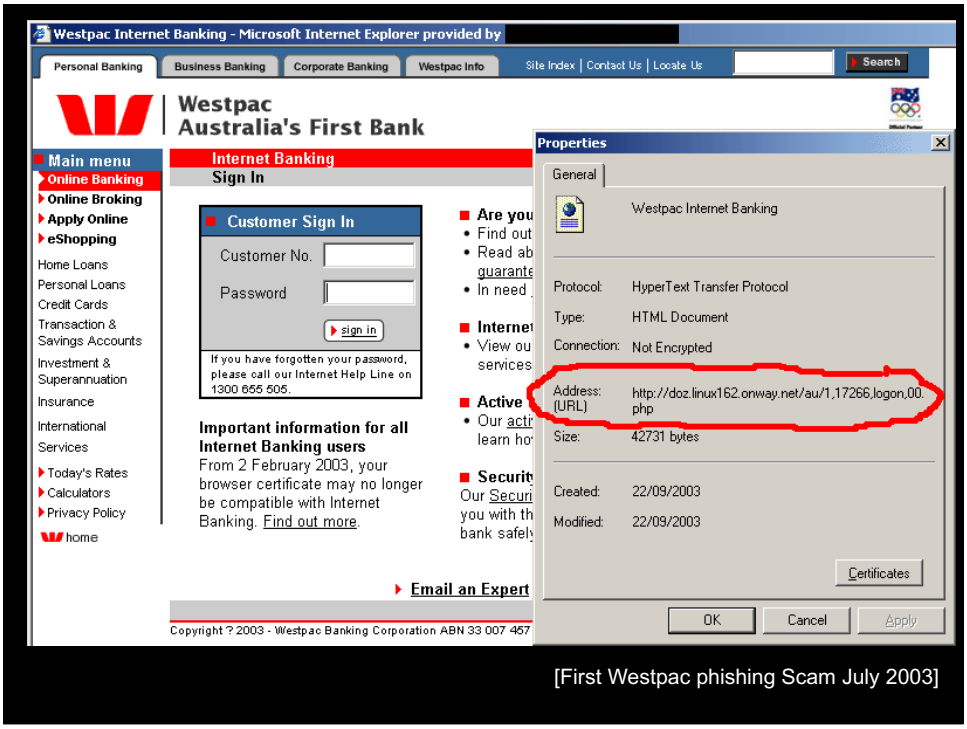
" If customers receive an email requesting security information they should delete it. Customers should not provide their personal security information via a link in an email."

Anyone who wants to change their internet banking password should contact the bank on 1300 655 505.

The bank says it "is working with other authorities such as the Australian Federal Police to stop this activity".

[First Westpac phishing Scam July 2003]

24



[First Westpac phishing Scam July 2003]

25

The Internet .. and disconnects

Slide 26

The environment is changing

- The frequency, scale, sophistication and severity of cyber incidents, both ***state sponsored*** and ***cybercriminal*** *rising*
- More diverse and innovative attempts to compromise government and private sector networks.
- observed multiple compromises after initial disclosure Microsoft Exchange and Accellion File Transfer Application (FTA))
- Cybercriminal sophistication and deliberate targeting
- Foreign states increasing their level of investment in cyber capabilities

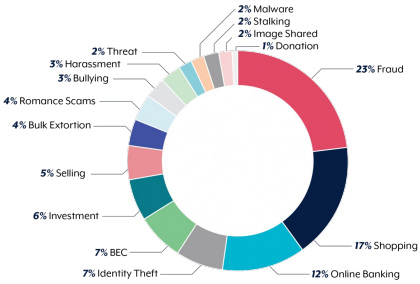
  Australian Cybersecurity Centre Report 2021-2022

26

The Internet .. and disconnects

Slide 27

Of concern in the Australian cybersecurity centre

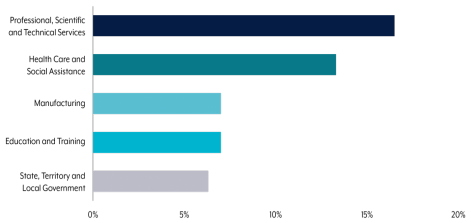


Cybercrime reports by type for financial year 2020–21

Domestic

Institutional

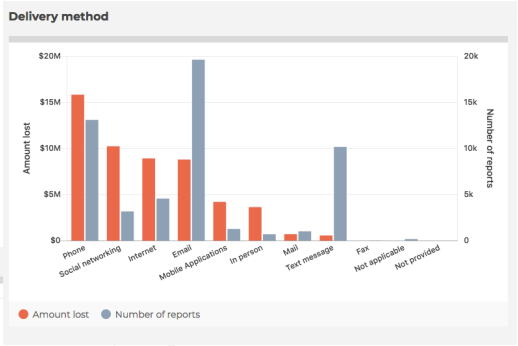
Top five reporting sectors for ransomware-related cyber security incidents

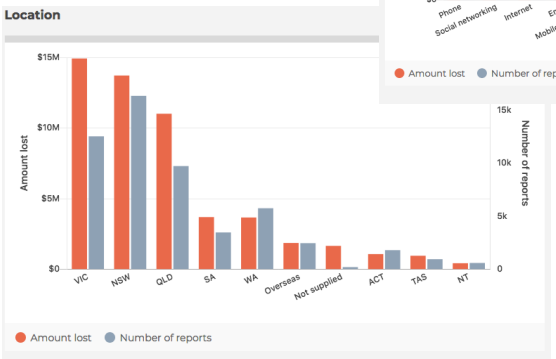


27

Phishing

A growing problem





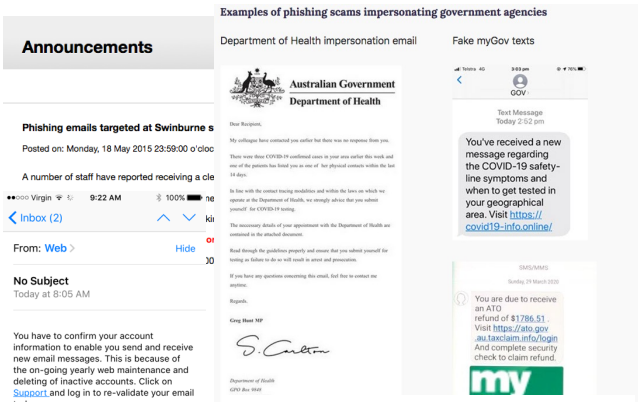
Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email, but increasing text messaging. The goal is to steal sensitive data like credit card and login information, gain permissions, or to install malware on the victim's machine.

28

Phishing

Slide 29

A growing problem



Scamwatch received over 4560 coronavirus-related scam reports with over $5,118, 000 in reported losses since the outbreak. Common are phishing for personal information, government and financial assistance on offer, online shopping, and superannuation (early access) scams.

29

Phishing

Slide 30

A growing problem

Showing All scam types stats for 2020

Amount lost	Number of reports	Reports with financial losses
$52 971 358	53 904	13.2%

$101,522,744 – 12.5%

30

Phishing

Slide 31

A growing problem

"Scammers are using pressure and fear tactics combined with technology to trick people into parting with their money,

Scammers increasingly ask for money via iTunes cards, Google Play cards and cryptocurrencies to avoid the anti-scam measures employed by banks and money laundering detection systems.

"Scammers are using COVID-19 as an excuse to divert your usual account payments to a different bank account. Your payment goes to the scammer instead of the real business."

Australian businesses are also being targeted by sophisticated 'business email compromise scams' with reports of losses to Scamwatch and other agencies exceeding $60 million in 2021.

Scammers are hacking businesses' email systems and impersonating key personnel in emails. They request changes to regular bank account details so that money is transferred to the scammer's account instead of where it should normally go. Many businesses are caught off guard because the emails appear genuine."

31

Phishing

Slide 32

Responses

- At the moment responses are largely inadequate and thwart, ***why?***
- **User education (especially in terms of spoofed links)**
- Two factor identification often not in place but increasing (more than one ID process required)
- Ways of detecting changes in IP addresses often not in place

An essential part of cybersecurity is assessing both the threats to the organization (information assets) as well as the vulnerabilities that exist within the organization's connected systems

32

Ransomware

Slide 33

A growing problem

- Encrypts files and folders, the affected are not unlocked until the ransom is paid
- First examples 1986-1989 'AIDS' Trojan aka PC-Cyborg
- 2013 Mac specific ransomware arrives and Cryptolocker work rakes in an estimated $5 million

2019 Telstra Security Survey of 1300 IT Security decision makers , 52% of those surveyed had experienced a ransomware incident and half of those had paid

Ransomware

Slide 34

Responses

- No More Ransomware (https://www.nomoreransom.org/), law enforcement agencies (led by The Netherlands) and IT Security companies (e.g. Kapersky & Intel) have joined forces to disrupt cybercriminal. Reporting, Decryption software, Awareness

1. Back-up! Back-up! & Back-up!
2. Use robust antivirus software to protect your system from ransomware.
3. Keep all the software on your computer up to date.
4. Trust no one. Manage awareness
5. Enable the 'Show file extensions' option in the Windows settings on your computer. This will make it much easier to spot potentially malicious files. Stay away from file extensions like '.exe', '.vbs' and '.scr'.

Risk assessment Vs. BIA

Slide 35

Informing Incident Response

One of the fundamental differences between risk management & BIA is that risk management focuses on identifying the threats and vulnerabilities to information assets in order to determine which controls can protect the information

The BIA assumes that these controls have been bypassed, have failed, or have otherwise proved ineffective, that the attack succeeded, and that the adversity that was being defended against has been successful. *Thus, we now focus on evaluating impacts on mission critical areas of the business*

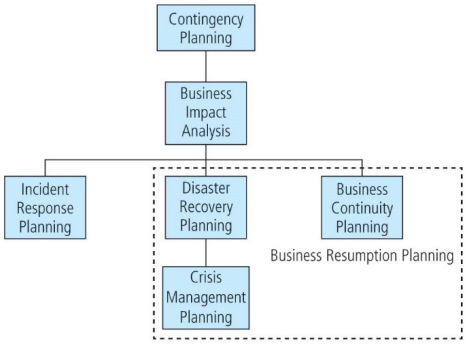


Figure 10-1 Contingency planning hierarchies

Business continuity management

Slide 36

Business continuity planning and incident response

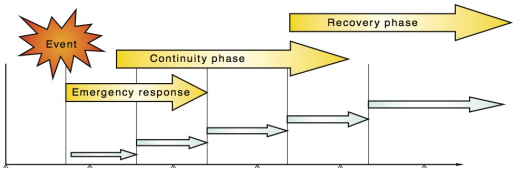
- Business continuity planning: is about providing a platform (or enterprise wide framework) for those activities intended to ensure the ongoing running of an organisation during the period of disruption of normal operation (in the face of an event)
  - Incident response: focuses on immediate information systems security responses to incidents affecting systems and networks
  - Disaster recovery refers to those activities required to minimize the the disruption on the organization and recover from a loss, either short or long term, especially in terms of information processing facilities
- Preventative controls are never 100% effective so controls must be in place to mitigate the effects once a disruption has occurred
- Control planning must be based on the assumption that any information system is subject to multiple types of failures.
- Procedures must exit and must be tested for recovery from failures, losses of equipment, applications and data

BCM and Contingency planning

Slide 37

Planning for incident response

The identification and prioritization of a response and recovery process



HB292-2006 – A Practitioners Guide to Business Continuity Management

Most organizations have experience detecting, reacting to, and recovering from attacks, employee errors, service outages, and small-scale natural disasters, and are thus performing incident response (IR)

The incident response plan (IR plan) is usually activated when the organization detects an incident that affects it, regardless of how minor the effect is

A formal program that prepares an entity for an incident.

37

Swinburne

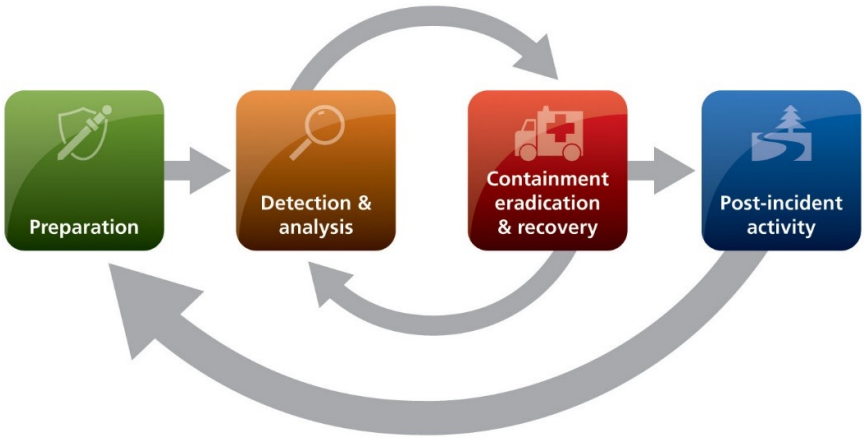


Figure 10-6 NIST incident response life cycle

Source: NIST Special Publication 800-61, Rev. 2: The Computer Security Incident Handling Guide.

38

BCM and Contingency planning

Slide 39

IR Actions, planning

- We've completed the planning (through Governance, Risk Management, Business Impact Assessment
- Incident response actions can be organized into three basic phases:
  - Detection
  - Reaction
  - Recovery
- Post incident assessment

A formal program that prepares an entity for an incident.

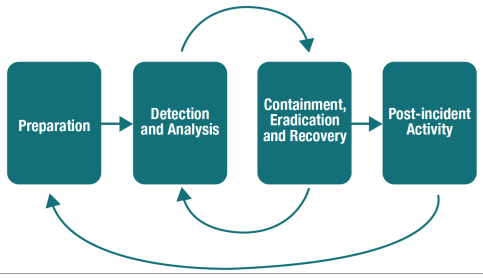
39

BCM and Contingency planning

Slide 40

1. Preparation to *establish roles, responsibilities and plans* for how an incident will be handled
2. Detection and Analysis *capabilities to identify incidents as early as possible and effectively* assess the nature of the incident

Figure 6—Incident Response Phases



3. Audit and Investigation capabilities where identifying an adversary (threat to information assets) is required
4. Mitigation and Recovery develop procedures to contain the incident, reduce losses and return operations to normal
5. Post-incident Analysis to determine corrective actions to prevent similar incidents in the future

ISACA Cyber security fundamentals (CSX)

40

BCM and Contingency planning

Slide 41

Preparation (Preparation)

- Occurs long before an incident actually happens.
- Establish policies for handling incidents (responsibilities, communications and approaches to emergency response, continuity and recovery… *for scenarios*)
- Establish incident response team (undertake rehearsals, tests and exercises – *see HB292*)
- Develop relationships with law enforcement and other entities, such as Internet service providers (ISPs), that may be involved in the incident response plan (e.g. Crisis communications planning).
- Establish and confirm preventative controls including the acquisition of the forensics tools and skills needed to investigate an incident.
- **During preparation, an organisation should prepare for and implement controls on systems, establish baselines and perform risk assessments**.

41

BCM and Contingency planning

Slide 42

Activating the response (Detection and analysis)

- Isolate threats, events. Not all cyber incidents will be emergencies or self evident and may be detected from a variety of sources, including reports from end users, administrators and external entities. Similarly, they may be triggerered by an alarm from intrusion detection systems (IDSs) or log management software.
- Once incident occurs/ & is detected, incident response team should analyze the information available to determine action and resourcing correlation and external resources. Note this can be about gathering forensic evidence, establishing a chain of custody documenting each person involved in handling the evidence.
- **Activating and deploying your response, intelligence and planning, administration, communications and logistics**

42

BCM and Contingency planning

Slide 43

Recovery (Containment and eradication)

- limit the amount of damage the attacker can cause as well as preserving evidence. This may include moving the machine to an isolated Virtual local area network (VLAN) or disconnecting it from the network to prevent it from affecting other systems and to disrupt the attacker's control.
- Establish forensic evidence
- Clean up systems check for new vulnerabilities. After the system has been restored, recovery takes place by reinstating the services the system provided (understanding MAO, MTD, RTO, RPO).
- as new information is discovered, the incident handler should identify and analyze this information and act appropriately.
- **Based on your recovery objectives / metrics – focusing on returning to routine operation)**

IR Planning

Swinburne

For every disruption scenario, Incident Response Planning can create three sets of incident-handling procedures:

1. During the incident
2. After the incident
3. Before the incident

Once these sets of procedures are clearly documented, the IR portion of the IR plan is assembled, and the critical information outlined in these planning sections is recorded

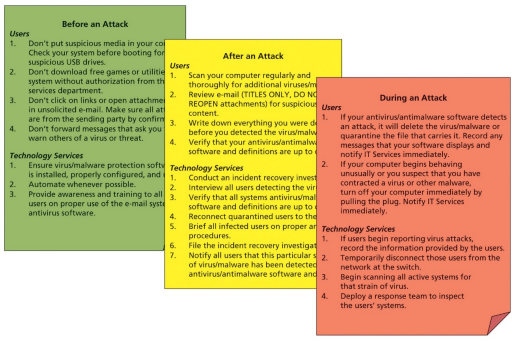


Figure 10-8 Example of IRP incident-handling procedures

- Planning requires a detailed understanding of the information systems and the threats they face
- Develop predefined responses that will guide the response team and users through the IR steps
- Predefining incident responses enables rapid reaction without confusion or wasted time and effort

Swinburne

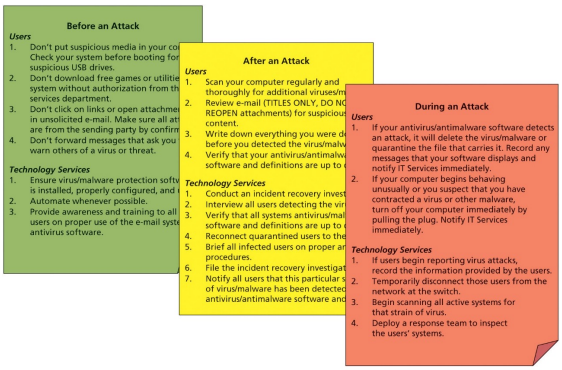


Figure 10-8 Example of IRP incident-handling procedures

Whitman Chapter 10 provides examples that you can use to model your own Incident Responses with

45

BCM and Contingency planning

SWIN BUR NE Slide 46

Assessing (post incident activity)

- primarily about lessons learned.
- The incident handling team should document the results of the investigation as well as the steps taken.
- Not only should the incident itself be reviewed,
- the processes and performance of the incident team should be reviewed as part of a continuous improvement process.
- This is an internal control

46

Swinburne

Documenting the incident

Table 10-2 Incident Handling Checklist from NIST SP 800-61, Rev. 2

	Action	Completed
	Detection and Analysis	
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
	Containment, Eradication, and Recovery	
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
	Post-Incident Activity	
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)[a]	

[a]While not explicitly noted in the NIST document, most organizations will document the findings from this activity and use it to update relevant plans, policies, and procedures.

Source: NIST SP 800-61, Rev. 2.

47

Thank you

Bring your questions to or face to face class

SWINBURNE UNIVERSITY OF TECHNOLOGY

Swinburne think forward

48