THE UNIVERSITY OF MELBOURNE

INFO30006
Information Security and Privacy

Week 02: Information Security Practices

Dr Heidi Tscherning

Today's session

1. WHAT IS INFORMATION SECURITY?
2. CHANGING INFORMATION SECURITY THREAT LANDSCAPE
3. INFORMATION SECURITY PROTECTION AND CONTROLS
4. THE BIGGER PICTURE
5. FINAL REMARKS AND WORKSHOP 02

Today's session

1. WHAT IS INFORMATION SECURITY?
2. CHANGING INFORMATION SECURITY THREAT LANDSCAPE
3. INFORMATION SECURITY PROTECTION AND CONTROLS
4. THE BIGGER PICTURE
5. FINAL REMARKS AND WORKSHOP 02

Stephen Colbert on security

Source: Kelley, H 2014, Stephen Colbert gives controversial security conference talk', CNN, 3 March 2014: http://edition.cnn.com/2014/03/01/tech/colbert-rsa-keynote/index.html and https://youtu.be/UsaXEKtLehs

Information security and privacy headlines

WIRED

The Apple-FBI Fight Isn't About Privacy vs. Security. Don't Be Misled

upporter | subscribe | search | events | Australia edition

theguardian

politics | sport | football | culture | lifestyle | environment | economy | media | tech | travel | browse all sections

Darknet sale of Medicare data 'traditional criminal activity', minister says

Alan Tudge downplays Guardian Australia's revelations and declines to answer questions about the breach

The Medicare machine: patient details of 'any Australian' for sale on darknet

E D

To Fix Voting Machines, Hackers Tear Them Apart

SHARE

SHARE 327

TO FIX VOTING MACHINES, HACKERS TEAR THEM APART

Biggest Cyber Security Threats To Australian

sation safe.

ted 08/04/2017 8:38 PM AEST

SHARE

SHARE 709

TWEET

COMMENT

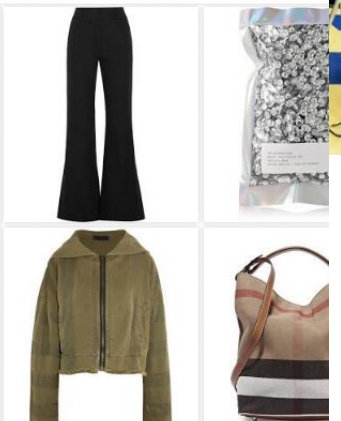
EMAIL

BRIAN BARRETT SECURITY 01.18.16 07:00 AM

WHEN GOOD DRONES GO BAD

Libby-Jane Charleston

Associate Editor, HuffPost Australia



What are assets, threats, vulnerabilities, and risks?

What is an **asset**?

An asset is what we're trying to protect.

People, property, information.

What is a **threat**?

A threat is what we're trying to protect against.

Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

What is a **vulnerability**?

A vulnerability is a weakness or gap in our protection efforts.

Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.

What is a **risk**?

Risk is the intersection of assets, threats, and vulnerabilities.

The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

Assets, threats, vulnerabilities, and risks in context

	CITIZENS/CONSUMERS	BUSINESSES	NATIONS
Asset			
Threat			
Vulnerability			
Risk			

Assets, threats, vulnerabilities, and risks in context

	CITIZENS/CONSUMERS	BUSINESSES	NATIONS
Asset	Information about: • Behaviours • Locations • Habits etc.		
Threat	• Legislative policies weakening consumer rights; e.g. consumer laws • Extortion		
Vulnerability	• Lack of knowledge: legislation and political affairs • Non-encrypted information		
Risk	• Loss of privacy / finances • Human capability no longer available		

Assets, threats, vulnerabilities, and risks in context

	CITIZENS/CONSUMERS	BUSINESSES	NATIONS
Asset	Information about: • Behaviours • Locations • Habits etc.	• Competitive knowledge • Sensitive information; e.g. ground-breaking smartphone design	
Threat	• Legislative policies weakening consumer rights; e.g. consumer laws • Extortion	Hacking, phishing, pressure from governments, malicious employees, human error, espionage, technological obsolescence	
Vulnerability	• Lack of knowledge: legislation and political affairs • Non-encrypted information	• Lack of risk management process • Lack of protection mechanisms for protecting assets	
Risk	• Loss of privacy / finances • Human capability no longer available	• Lack of security management process/documentation • Poor internal security policies and culture amongst employees	

Assets, threats, vulnerabilities, and risks in context

	CITIZENS/CONSUMERS	BUSINESSES	NATIONS
Asset	Information about: • Behaviours • Locations • Habits etc.	• Competitive knowledge • Sensitive information; e.g. ground-breaking smartphone design	
Threat	• Legislative policies weakening consumer rights; e.g. consumer laws • Extortion	Hacking, phishing, pressure from governments, malicious employees, human error, espionage, technological obsolescence	
Vulnerability	• Lack of knowledge: legislation and political affairs • Non-encrypted information	• Lack of risk management process • Lack of protection mechanisms for protecting assets	
Risk	• Loss of privacy / finances • Human capability no longer available	• Lack of security management process/documentation • Poor internal security policies and culture amongst employees	

Now over to you!

Our initial definitions…

Information security

is about defending information: *preventing unauthorised access, use, disclosure, disruption, modification, inspection, recording or destruction of information.*

Privacy

is about safeguarding personal data and protecting a personal image through e.g. encryption and decryption of data.

The safeguarding of personal data is the objective; i.e. data about individuals, such as contact information, health, financial, and family information; these individuals could be employees, your customers and other stakeholders. There are various legal, regulatory, political, and technological issues surrounding the issue of data privacy.

Cryptography

Enables secure information transactions by encryption/decryption of data.

Today's session

1. WHAT IS INFORMATION SECURITY?
2. CHANGING INFORMATION SECURITY THREAT LANDSCAPE
3. INFORMATION SECURITY PROTECTION AND CONTROLS
4. THE BIGGER PICTURE
5. FINAL REMARKS AND WORKSHOP 02

Threats to information security

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

Source: Whitman, ME & Mattord, HJ 2012, Principles of information security, Boston, MA, USA, p. 44

Threats to information security

Question:

How do these information security threats act in an organisations?

Threats to information security

1. **Human error or failure: What is human error?**
   - Employee mistakes: revelation of classified data, failure to protect information, etc.
2. **Compromises to intellectual property (IP): What is IP?**
   - Software piracy, copyright infringements etc.
3. **Deliberate acts of espionage or trespass: What forms can espionage take?**
   - Unauthorised access and/or data collection:
     - Competitive or industrial espionage
     - Hacking and shoulder surfing

What does a hacker look like…?

Exercise:

Discuss in small groups, what “Cybercriminals” look like today:
(Threat category of deliberate espionage and trespass)

- What do they “look like”?
- What are their motives?
- What are different types/levels of hackers?

Threats to information security

4. **Deliberate acts of information extortion: who and how?**
   - Attacker steals information from computer system and demands compensation for its return or nondisclosure: RansomWare: iCloud leak of sensitive celebrity photos
5. **Deliberate acts of sabotage or vandalism: motives?**
   - Software vandalism etc.: Hacktivists – petty vandalism, more serious: cybercriminals, nation state hackers
6. **Deliberate acts of theft: examples?**
   - Illegal taking of another's physical, electronic, or intellectual property
7. **Deliberate software attacks: examples?**
   - Malicious software, such as viruses, worms, Trojan horses, back doors etc.
8. **Forces of nature**
   - Bush fire, flooding, earthquakes etc.

Threats to information security

9. **Deviation of service: such as?**
   - Internet service, communications, and power irregularities
10. **Hardware failure**
   - Distribution by manufacturer
11. **Software failure**
   - Software which is faulty, contains bugs
12. **Technical obsolescence**
   - Outdated infrastructure, technology that becomes obsolete

Changing information security landscape

Last decade has seen a global shift in terms of information security threats in the media causing information security to become a main concern for businesses and nations: Video: The new Cyber threat:

NB! Added slide 5 August 2017, discussed in Week 03: Management of security risks

Changing information security landscape – examples

- 2015: US filing cyber espionage charges against Chinese military
- 2013: Snowden reveals US hackers targets China, North Korea, Hong Kong
- 2013: US charged Russian/Ukranian hackers with hacking into computers of major retailers, payment processors and banks stealing customers' credit card numbers.

NB! Added slide 5 August 2017, discussed in Week 03: Management of security risks

Today's session

1. WHAT IS INFORMATION SECURITY?
2. CHANGING INFORMATION SECURITY THREAT LANDSCAPE
3. INFORMATION SECURITY PROTECTION AND CONTROLS
4. THE BIGGER PICTURE
5. FINAL REMARKS

Information security controls

Information security ‘best-practice’ suggest a range of managerial and technical controls to protect information resources:

1. Information security ***risk management***
2. Information security ***policy***
3. Information security ***strategy***
4. Information security ***education, training and awareness (SETA)***

Information security risk management

What is security risk management?

The level of security risk exposure must guide an organisation's selection of *controls*.

- Risk identification
- Risk assessment
- Risk response
- Risk review/control

We will discuss information security risk management in Week 03!

Information security policy

What is a security policy?

"A policy is a plan or course of action that conveys instructions from an organisation's senior management to those who make decisions, take actions, and perform other duties".

The term 'policy' may refer to strategic-level guidance or operational-level guidance. Other terms we may use are 'practices' and 'procedures'.

We will discuss information security risk management in Week 09!

Source: Whitman, ME & Mattord, HJ 2012, Principles of information security, Boston, MA, USA, p. 177

Information security strategy

What is a security strategy?

Strategy prescribes a future course of security actions to be enacted upon using a range of formal, informal and technological controls at a tactical and operational level in order to reduce security risk exposure (i.e. risks to confidentiality, integrity and availability). Strategy is:

- *prescriptive* in that it involves decision-making about a future course of action
- *multi-faceted* and incorporates trade-offs

We will discuss strategy in Week 10

Information security education, training, awareness (SETA)

What is a SETA?

SETA is designed to positively influence the security behaviours of employees.

SETA:

- is a control measure designed to influence security behaviours of employees.
- draws its aims and objectives from security policy and security strategy.
- When an organisation has conducted a comprehensive security risk assessment, a critical aspect of crafting the risk mitigation strategy is to determine how to use SETA to complement formal controls (e.g. policy) and technical controls (e.g. firewalls and anti-virus software).

Today's session

1. WHAT IS INFORMATION SECURITY?
2. CHANGING INFORMATION SECURITY THREAT LANDSCAPE
3. INFORMATION SECURITY PROTECTION AND CONTROLS
4. THE BIGGER PICTURE
5. FINAL REMARKS AND WORKSHOP 02

The bigger picture

Information security threats

1. Human error or failure:
2. Compromises to intellectual property (IP)
3. Deliberate acts of espionage or trespass
4. Deliberate acts of information extortion
5. Deliberate acts of sabotage or vandalism
6. Deliberate acts of theft
7. Deliberate software attracts
8. Forces of nature
9. Deviations in quality of service form provider
10. Technical hardware failure or virus
11. Technical software failure or virus
12. Technological obsolescence

Information security controls

1. Risk
2. Policy
3. Strategy
4. Security education, training, awareness

Today's session

1. WHAT IS INFORMATION SECURITY?
2. CHANGING INFORMATION SECURITY THREAT LANDSCAPE
3. INFORMATION SECURITY PROTECTION AND CONTROLS
4. THE BIGGER PICTURE
5. FINAL REMARKS AND WORKSHOP 02

Why care about information security…?

We have been exposed you to a range of security threats and attacks. You have been asked to consider examples that might take place in your own organisation and what countermeasures might be applicable. And we have made you aware of a number of information security controls.

Workshop 02:

Task:

1. Watch: Four Corners – Weapons of mass surveillance (see workshop information on LMS!)
2. Answer three questions as preparation for next week's workshop
3. Check who will be presenting and facilitating the workshop next week – Check Groups for workshop: overview on LMS