


MONASH
University

MONASH
BUSINESS
SCHOOL

Ethics in AIS, Fraud & Cybercrime
Additional Reading – Romney et al. (2013)
pages 21-24)
Romney and Steinbart (2018) - Chapter 5 &
Chapter 6

Chief Examiner Edward Tello
Semester 2, 2018

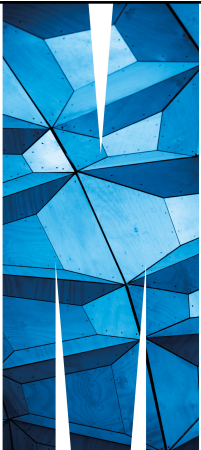
COMMONWEALTH OF AUSTRALIA
Copyright Regulations 1969
WARNING

This material has been reproduced and communicated to you by or on behalf of Monash University pursuant to the Copyright Act 1968 (the Act). The material in this communication may be subject to copyright under the Act. Any further reproduction or communication of this material by you may be the subject of copyright protection under the Act.

Do not remove this notice.





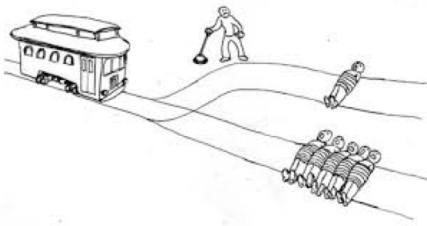


Introduction to Ethics
Romney et al. (2013), pp. 21-25 (see
'Reading List' on Moodle - Week 3)





Ethical Dilemma ...





Ethical Dilemma

- What is the morally right thing to do?

You are on a country road and see 2 neighbouring farm houses on fire. One is yours and the other belongs to a new couple who just moved in. Your wife and child are at home as are your neighbours. You can only save one house. Which one do you save?

- According to Allen (2012), 3 conditions must be present for a situation to be considered an ethical dilemma:

- 1) The first condition occurs in situations when an individual, called the "agent," must make a decision about which course of action is best
- 2) There must be different courses of action to choose from
- 3) No matter what course of action is taken, some ethical principle is compromised. In other words, there is no perfect solution



What does Ethics involve?



Ethics

- Ethics is generally considered to deal with relations of humans to each other (Gilbert, 2012 – see **Reading List**)
- One way to describe the field of ethics is that it deals with those actions affecting other people that make us feel good or bad about ourselves (Gilbert, 2012 – see **Reading List**)
- Ethics are propositional statements (standards) that are used by members of a profession or group to determine what the right course of action in a situation is (Allen, 2012)
- Ethics rely on logical and rational criteria to reach a decision, an essentially cognitive process



Ethics

The central question of ethics is:
'what ought one to do?'

Ethics is about making a choice or good decision. Ethics is how we act to make the 'right' choice and produce 'good' behaviour

Source: Parkes et al. (2016)



Ethical Issues in Accounting

- In every instance, ethical judgments boil down to a personal decision:

What should I do in a given situation?

- The nature of the work carried out by accountants and auditors requires a high level of ethics (Verschoor, 2017)
- Knowledge of ethics can help accountants & auditors to overcome ethical dilemmas, allowing for the right choice that, although it may not benefit the company, will benefit the public who relies on the accountant/auditor's reporting

Source: Verschoor, 2017 – Accounting Today (see **Reading List** on Moodle – recommended / voluntary)



Ethics and Managers

- Corporate decisions are made by **managers** → Decisions of managers do affect other people
- Milton Friedman → NY Times 1970 → **"The social responsibility of business is to increase its profits"**
- In reaction to Friedman's article → Professor R.E. Freeman → Corporations and their managers have **responsibilities to their stakeholders**
- Managerial Ethics must of necessity **examine the impacts of the actions of managers**
 - Not just compliance or non-compliance of those actions with laws and regulations

Source: Gilbert (2012 pp. 36-40), "Ethics for Managers" (see **Reading List** on Moodle - recommended)



How to make an ethical decision?

Ethical Decision-Making Framework

- Answering these 4 questions will guide you through tough decisions:
 - 1) Is there an ethical situation or dilemma?
 - 2) Move to a resolution by identifying elements of the problem:
 - What parties (stakeholders) may be harmed?
 - Whose rights or claims may be violated?
 - Which specific interests are in conflict?
 - What are my responsibilities and obligations?

Source: Romney et al. (2013) (see [Reading List](#) on Moodle - [required](#))



How to make an ethical decision?

Ethical Decision-Making Framework

- Answering these 4 questions will guide you through tough decisions:
 - 3) Specify alternatives and weigh up impacts of each on various stakeholders
 - 4) Select best or most ethical alternatives considering all circumstances and consequences



Ethical analysis (example): Enron case



- David Duncan, the lead auditor of Enron Corporation, [thinks Enron is understating the liabilities on its balance sheet](#)
- Enron's transactions are complex, and outsiders may never figure this out. Duncan asks [his firm's Standards Committee](#) how he should handle the situation. They reply: '[Require Enron to report all its liabilities](#)'

Source: Romney et al. (2013) (see [Reading List](#) on Moodle - [required](#))



Ethical analysis (example): Enron case



- Enron is Duncan's most important client, and Enron is pressuring him to certify liabilities
- Duncan can rationalise that Enron's reported amounts are OK. What should he do?



Ethical analysis (example):
Enron case

1) What is the ethical issue?

- ???????



Ethical analysis (example): Enron case

2) What are the principle elements?

a) Who may be harmed?

- Duncan, Duncan's firm, investors, creditors, possibly employees if the understatement is large, the auditing profession as a whole

b) Whose rights/claims may be violated?

- Investors, creditors



c) Which interests are in conflict?

- ✓ Enron's interest in having its accounts certified with a 'clean' opinion is potentially in conflict with **Duncan's obligations, professional code of Ethics, and investors, financiers & creditors**
- ✓ Duncan's professional obligations are in conflict (**as an auditor and as a partner**)
- ✓ The firm's interests are in conflict with the **Standards Committee**



d) What are your (or the focal character's) responsibilities and obligations?

- ✓ Duncan is bound by his firm's rules (the standards committee has given him clear advice)
- ✓ Duncan also bound by the code of ethics of his professional organisation
- ✓ Legally and morally, Duncan has a duty of care that extends beyond his relationship with Enron. Includes duty to:
 - ✓ Colleagues,
 - ✓ Shareholders of the firm,
 - ✓ Firm's creditors, employees,
 - ✓ Even the wider communities that are involved with Enron and its auditors



Ethical analysis (example): Enron case



3. What options exist and what are the consequences?



Ethical analysis (example): Enron case

4. What is the most ethical course of action?

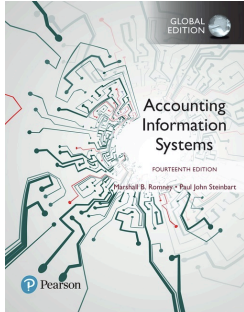
Forcing Enron to re-state liabilities is the most ethical course of action here

What did Duncan actually do?

Went against his firm's advice, certified Enron's liabilities

MONASH University

Chapter 5
Fraud
Romney and Steinbart (2018)



MONASH University

Learning Objectives

- Explain the threats faced by modern information systems
- Define fraud and describe both the different types of fraud and the auditor's responsibility to detect fraud
- Discuss who perpetrates fraud and why it occurs, including the pressures, opportunities, and rationalizations that are present in most frauds
- Define computer fraud and discuss the different computer fraud classifications
- Explain how to prevent and detect computer fraud and abuse

MONASH University

Is there any relationship
between Fraud & Ethics?





Opening Case: The Enron scandal



- The Enron scandal (publicised in October 2001) eventually led to the bankruptcy of the Enron Corporation (an American energy company based in Texas)
- It also led to the de facto dissolution of Arthur Andersen (1 of the 5 largest audit and accountancy partnerships in the world)
- As a result, the rules for company financial reporting were drastically sharpened (Sarbanes-Oxley Act (2002))





...but it is not the only case involving
the accounting profession!!

Ethics in Accounting in a "must"



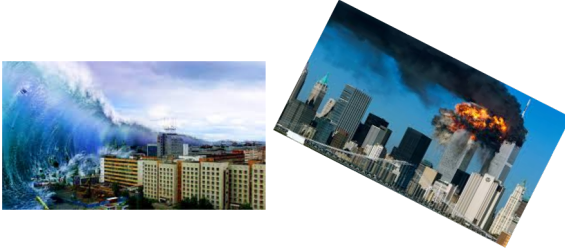






Threats to Accounting Information Systems

- **Natural and Political disasters**



A valid concern is about what is going to happen when cyberattacks are militarised

MONASH University

Threats to Accounting Information Systems

- **Software errors & equipment malfunctions**



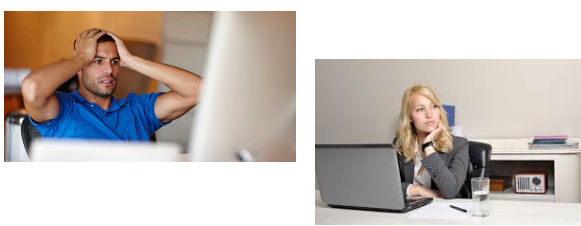
- Yearly economic losses due to software bugs is almost \$60 billion
- More than 60% of companies studied had significant software errors

MONASH University

Threats to Accounting Information Systems

- **Unintentional acts**

- Human errors cause 80% of security problems (Source: Computing Technology Industry Association)



MONASH University

Threats to Accounting Information Systems

• Intentional acts



Cyber thieves have stolen more than \$1 trillion worth of intellectual property from businesses worldwide

What is Fraud??

Gaining an unfair advantage over another person

Legally, an act must be:

- A false statement, representation, or disclosure
- A material fact that induces a person to act
- An intent to deceive
- A justifiable reliance on the fraudulent fact in which a person takes action
- An injury or loss suffered by the victim

Individuals who commit fraud are referred to as **white-collar criminals**



Typically, they are businesspeople & government professionals who commit fraud

Two Categories of Fraud (important to businesses)

• Misappropriation of assets

- Theft of company assets by employees which can include physical assets & digital assets



What are the most significant factors in most misappropriation of assets?

- ??????



Two Categories of Fraud (important to businesses)

• Fraudulent financial reporting

- “cooking the books” (e.g., booking fictitious revenue, overstating assets, etc.)



‘...intentional or reckless conduct, whether by act or omission, that results in materially misleading financial statements’
(The Treadway Commission)

Auditor's Responsibility

- SAS No. 99 (AU-C Section 240) requires auditor's to:
 - ✓ Understand fraud
 - ✓ Discuss the risks of material fraudulent misstatements
 - ✓ Obtain information
 - ✓ Identify, assess, and respond to risks
 - ✓ Evaluate the results of their audit tests
 - ✓ Document and Communicate findings
 - ✓ Incorporate a technology focus

In Australia we follow the Auditing Standard ASA 240 prepared by the AASB:

www.aasb.gov.au/admin/file/content102/c3/Nov13_Compiled_Auditing_Standard_ASA_240_1502324015481.pdf



Which one is the criminal?



KPMG: 'Global profiles of the fraudster' 2016 report

- The report is based on an analysis of 750 fraudsters across 81 countries:
 - between the ages of 36 and 55
 - predominantly male, with the proportion of women on the rise at 17%, up from 13% in 2010
 - a threat from within
 - holds an executive or director level position
 - employed in the organization for at least six years
 - described as autocratic & 3 times as likely to be regarded as friendly as not
 - esteemed, describing themselves as well-respected in their organization
 - likely to have colluded with others
 - motivated by personal gain, greed & the sense of 'because I can'

Source: KPMG

<https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf>



Fraud Triangle: Conditions for fraud

- These 3 conditions must be present for fraud to occur:

The diagram is a pink triangle divided into three sections:

- Incentive/Pressure**
(Motivation for fraud)
- Rationalisation**
(Ethics, values, character deficiencies)
- Opportunity**
(circumstances enabling fraud: Commit, Conceal, Convert to personal gain)

MONASH University

Computer Fraud

- If a computer is used to commit fraud it is called computer fraud
- Computer Fraud Classifications:

The diagram shows five pink boxes arranged in a circle:

- Input fraud
- Processor fraud
- Output fraud
- Data fraud
- Computer instructions fraud

MONASH University

Read pages 166-168 for some examples of each

Preventing and Detecting Fraud

- How???

A blue box with the text "???" is on the left. A blue circular icon with a white question mark is on the right.

MONASH University

Read the following case of employee fraud, make 2 recommendations to prevent similar problems in the future (how to improve its control system?):

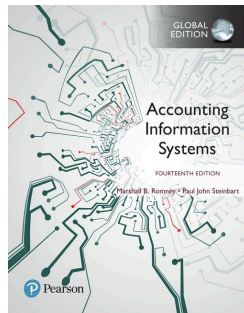


Some customers found that the products of a prestigious German brand sold at retail shops in China are counterfeits. This explains why the customers prefer to buy those products in other countries. Investigation revealed that the staff of the retail shops exchange genuine products with fake ones. They sell the fake products to retail customers and the genuine ones through personal channels

• ?????



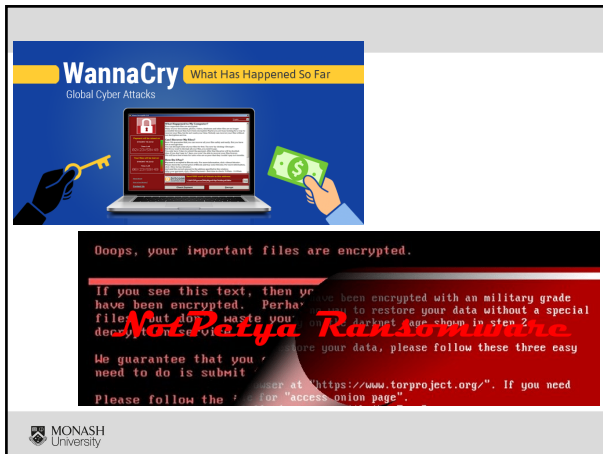
Chapter 6 Computer Fraud & Abuse Techniques Romney and Steinbart (2018)



Learning Objectives

- Compare and contrast computer attack and abuse tactics
- Explain how social engineering techniques are used to gain physical or logical access to computer resources
- Describe the different types of malware used to harm computers





Should Cybersecurity be a top priority for organisations?

- Recent major cyber attacks (such as the 2017 **WannaCry** or **NotPetya**) have been a wakeup call to many ... why?
 - ✓ They highlight the potentially widespread impact of a single cyber vulnerability & demonstrated the consequences of not taking cybersecurity seriously (Stephens, 2017)
- Many organisations still rely on out of date security solutions and haven't invested in security precautions (Stephens, 2017)
 - ✓ Few treat cyber as a strategic business risk

Cybersecurity is a "must" for companies, it should be at the forefront of decision making

- According to the **Ponemon Institute** in its '2015 Cost of Data Breach Study', on average it takes 46 days to resolve a cyber attack at an average cost of \$21,155/day, or a total cost of \$973,130
- In its '2017 Cost of Data Breach Study', the **Ponemon Institute** reports that in Australia data breaches cost companies an average of \$139 per compromised record & the total average cost paid by a company was \$2.51 million

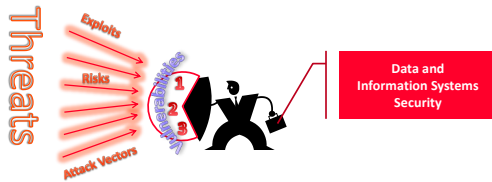


'If Data is Money, Why Don't Businesses Keep it Secure?'

- **Personal data is the new currency of the digital economy**
- Like money, personal data can flow easily across borders. Hot topics of debate include the ownership of data or the responsibilities of companies as custodians of data
- If businesses are to continue using personal data to create value for themselves & their customers, **they'll need to manage it carefully in 4 ways:**
 - Maintain trust to avoid data runs
 - Understand how regulation alters the data cost-benefit analysis
 - Manage brand reputation by engaging with data rating agencies
 - Strengthen customer sovereignty by learning from data intermediaries

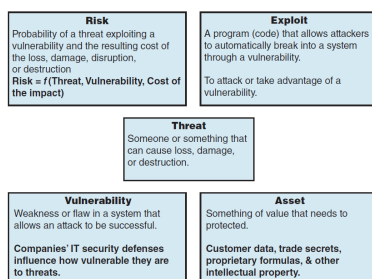
Source: Cooper et al., 2015 – HBR (see **Reading List** on Moodle – recommended / voluntary)

Basic IT Security Concepts



Source: Turban et al. (2015)

Basic IT Security Concepts



Source: Turban et al. (2015), "Information Technology for Management"

Types of Attacks

1) Computer Attacks and Abuse

- All computers connected to the internet are under constant attack from hackers, foreign governments, disgruntled employees, terrorist groups or competitors

2) Social Engineering

- Techniques or tricks on people to gain physical or logical access to confidential information

3) Malware

- Software used to do harm

These classifications are not distinct!!
There is a lot of overlap among the categories



1.1) Hacking



- Attacks to enter a system (steal or control resources)
- Accessing/using a computer system in an unauthorised manner. May involve modifying system.

?????



In the worst security data breach in history, 101 million Sony Play Station accounts were hacked crashing the network for over a month



Hacking

– Hijacking

- Gaining control of a computer to carry out illicit activities

– Botnet (robot network)

- Zombies
- Bot herders
- Denial of Service (DoS) Attack
- Spamming
- Spoofing



Botnets

- It's an attack to disable a system comprised of a collection of bots (or malware-infected computers)
- Those infected computers (called zombies) can be controlled and organized into a network of zombies on the command of a remote botmaster (called bot herder)



Source: How-To Geek (2016)

Denial-of-Service (DoS) Attack

- It is an attack to disable a system
- Constant stream of requests made to a web-server (usually via a Botnet) that overwhelms and shuts down service.



Spoofing

- It's an attack to enter a system (steal or control resources)
- It involves making an electronic communication look as if it comes from a trusted official source to lure the recipient into providing information



Forms of Spoofing



- E-mail spoofing
- Caller ID spoofing
- IP address spoofing
- Address Resolution (ARP) spoofing
- SMS spoofing
- Web-page spoofing (phishing)
- DNS spoofing



Hacking with Computer Code

- **Cross-site scripting (XSS)**
 - Uses vulnerability of Web application that allows the Web site to get injected with malicious code. When a user visits the Web site, that malicious code is able to collect data from the user
- **Buffer overflow attack**
 - Large amount of data sent to overflow the input memory (buffer) of a program causing it to crash and replaced with attacker's program instructions
- **SQL injection (insertion) attack**
 - Malicious code inserted in place of a query to get to the database information



Other Types of Hacking

- Man in the middle (MITM)
 - **Hacker is placed in between a client (user) and a host (server) to read, modify, or steal data**
- Masquerading/impersonation
- Piggybacking
- Password cracking
- War dialing and driving
- Phreaking
- Data diddling
- Data leakage
- Podslurping

Review them on pages 187 - 189



Hacking Used for Embezzlement

- **Salami technique:**
 - Taking small amounts at a time
 - Round-down fraud
- **Economic espionage:**
 - Theft of information, intellectual property, and trade secrets
- **Cyber-extortion:**
 - Threats to a person or business online through e-mail or text messages unless money is paid



Salami technique

- A type of computer fraud in which small amounts of money are transferred from numerous customer accounts into an account held under a false name (Oxford University Press, 2018)



Hacking Used for Fraud

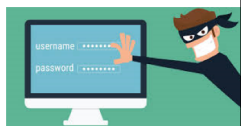
- Internet misinformation
- E-mail threats
- Internet auction
- Internet pump and dump
- Click fraud
- Web cramming
- Software piracy

Review them on pages 190 - 191

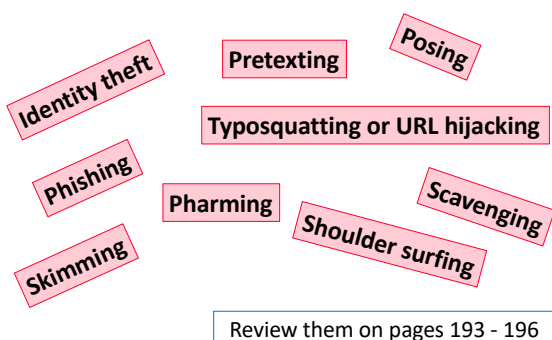


2) Social Engineering

- Also called **"human hacking"**
- Tricking users or abusing human social norms into gaining advantage to a system or asset illicitly or legally, such as gaining access to networks or accounts
- **Confidence tricks** (i.e. via interpersonal interaction) to gain access to sensitive data or information



Social Engineering Techniques



Phishing

- Deceptive method of stealing confidential information by pretending to be a legitimate organization or trusted source
- Messages include links to fraudulent phish websites that look like the real one

Source: Turban *et al.* (2015)



Spear Phishing

- Spear phishing attacks are highly targeted and customized so they are far more likely to succeed than traditional phishing attacks
- Spear phishers often target select groups of people with something in common

Source: Turban et al. (2015)



Why People Fall Victim

- | | |
|--|--|
| <ul style="list-style-type: none"> • Compassion <ul style="list-style-type: none"> – Desire to help others • Greed <ul style="list-style-type: none"> – Want a good deal or something for free • Sex appeal <ul style="list-style-type: none"> – More cooperative with those that are flirtatious or good looking • Sloth <ul style="list-style-type: none"> – Lazy habits | <ul style="list-style-type: none"> • Trust <ul style="list-style-type: none"> – Will cooperate if trust is gained • Urgency <ul style="list-style-type: none"> – Cooperation occurs when there is a sense of immediate need • Vanity <ul style="list-style-type: none"> – More cooperation when appeal to vanity |
|--|--|

Minimize the Threat of Social Engineering

- Never let people follow you into restricted areas
- Never log in for someone else on a computer
- Never give sensitive information over the phone or through e-mail
- Never share passwords or user IDs
- Be cautious of someone you don't know who is trying to gain access through you

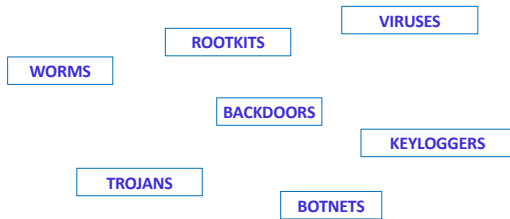
3) Malware

- Malware is an abbreviated term meaning “**malicious software**”
- This is software that is specifically designed to gain access or damage a computer without the knowledge of the owner (Symantec, 2017)



Malware

- Types of Malware:



Review them on pages 199 - 201

Malware

- Malware is not restricted to computers
- Recent viruses and worms have attacked cell phones and personal electronic devices
- Cellphone Bluetooth Vulnerabilities:
 - **Bluesnarfing:**
 - Stealing contact lists, data, pictures on bluetooth compatible smartphones
 - **Bluebugging:**
 - Taking control of a phone to make or listen to calls, send or read text messages

Cybersecurity



Business policies, procedures, training & Disaster recovery plans as well as hardware & software are critical to cybersecurity

