Week 1: Introduction

Fraud and cybercrime are evolving and contemporary crime categories. These crimes have significant impact on the financial and emotional wellbeing of victims, along with broader societal impact.
Current approaches to preventing, detecting and punishing these crimes have proven to be challenging.

- Governments, law enforcement and regulatory agencies attempt to combat their growing prevalence and sophistication of offender methodologies.

Evolution of Cybercrime
Cybercrime has been made possible by the rapid development and use of digital technology in modern life.
Technology has transformed the way in which we;

- Interact with friends and family; and
- Do business.

Technology can be used for 'good' and 'evil'

What are cybercrime offenders targeting? What is their purpose?

How can the following advances in technology be the subject of criminal exploitation?

- Sharing of photographs via social media - revenge porn, sharing of child pornography
- Online shopping - the black market, purchase of illegal goods and services
- Online government services such as submission of electronic tax returns - tax fraud

Elements of cybercrime
Modern cybercrimes are typically characterised by the following elements

- Organised;
- Financially motivated;
- Technologically sophisticated; and
- Transnational.

Emergence of cybercrime
Separate category of 'computer crime' as early as the 1960's.

- Reports of computer manipulation, computer sabotage, computer espionage and the illegal use of computer systems.
- Evolution of technology is matched to evolution of cybercrime offending
- Three 'generations' of cybercrime identified by Wall (2007)

Generation 1
The computer is used to *assist traditional offending*

- "Took place within discrete computing systems and was mainly characterized by the criminal exploitation of mainframe computers and their discrete operating systems"
- Target: acquisition of money or the destruction or appropriation of restricted information
    - Salami fraud is a good example of the first generation of cybercrime - Salami Slicing (or penny shaving) is the fraudulent practice of stealing money repeatedly in extremely small quantities, usually by taking advantage of rounding to he nearest cent (or other monetary unit) in financial transactions.
- Although this generation of cybercrime involves the use of the computer and sometimes, even the internet, these technologies are use to support traditional offences that predate them.

Generation 2
Committed across networks; crimes are 'hybrid'

- The internet has opened up new opportunities across global networks for traditional forms of criminal activities, such as a global trade in child pornography
- Trans-jurisdictional procedures are often required but may not be readily available - creates difficulties in addressing this generation of cybercrimes.

The global trade in pornography is a good example, because nations tend to have different standards on the legality of adult pornographic material.

- Activities become disconnected from place-based contexts and re-embedded in abstract systems - increasingly globally linked networks of computers.

Generation 3
The third generation of cybercrimes, 'true cybercrimes' are the product of opportunities *created* by the Internet.

- These criminal activities would not exist without the Internet
- 'Spamming' is a deviant act that has become an illegal act in many jurisdictions

These activities break the relationship between time and space - occur in virtual contexts of online communities

- Activities performed via text and other digital platforms, range from minor acts such as flaming (debates on message boards that are spelled in capital letters), to more serious crimes such as cyber rape; these activities can be described as deviant activities in cyber-communities

<u>Defining Cybercrime</u>
Many variations in terminology; broad consensus on three categories of cybercrime (US, Canada, UK and Australia)

- Cyber Dependent
- Cyber Enables
- Computer-Supported

Cyber Dependent

- "That can be committed using a computer, computer networks, or other form of ICT"
- Relates to offending where technology is the TARGET of the criminal activity
- Hacking, malware, DoS attacks

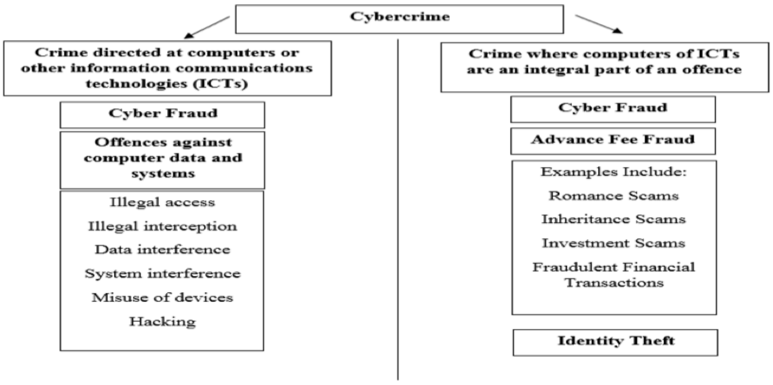
Cyber Enabled

- "Traditional crimes that are increased in their scale or reach by the use of computers, computer networks or other ICT"
- Child pornography, stalking, fraud
- These crimes are ENHANCED by technology; but can be committed without

Computer Supported

- Crimes in which the computer is an incidental aspect of the commission of the crimel may afford evidence of crime
- E.g. Addresses found in computer of murder suspect; google searches of 'how to dispose of a body'; text messages between drug dealers and clients

<u>Australian Cybercrime Act 2001</u>


Cybercrime
Crime directed at computers or other information communications technologies (ICTs)
Cyber Fraud
Offences against computer data and systems
Illegal access
Illegal interception
Data interference
System interference
Misuse of devices
Hacking
Crime where computers of ICTs are an integral part of an offence
Cyber Fraud
Advance Fee Fraud
Examples Include:
Romance Scams
Inheritance Scams
Investment Scams
Fraudulent Financial Transactions
Identity Theft

Cyber fraud offences (Australian Government Attorney-General's Department, 2013; *Cybercrime Act 2001).*

Technology as a 'Crime Enabler'

Scale

- Communication via the internet allows contact with many people, cheaply and easily
- 3 billion people with access to the internet, approximately 40 per cent of the world population; large pool of victims
- 'Force multiplier' - allowing offending to be committed on a scale that could not be achieved in offline environment
- The ability to automate certain processes further amplifies this effect. E.g. "Bredolab' botnet was estimated to have infected 30 million computers, generating 3 billion emails per day

Accessibility

- Technology is widely available and can be used without significant levels of expertise - by both offenders and victims
- US % of households with internet access increased from 18% in 1997 to 74.4% in 2013; Australia internet users = 84.6%
- Numbers of internet users in developing countries outnumbers developed countries
    - Why might this be a concern from a cybercrime perspective?

Anonymity

- Significant advantage for cybercrime offenders
- Deliberate concealment of identity
- Data can be routed through a number of jurisdictions - tracing is difficult
- Illegal access to wireless networks to conceal identity even if location is identified
- Jurisdictions identified that have poor regulation and oversight

Portability and Transferability

- 'Bid' data can be stored easily and cheaply
- Increase in technological capacity of devices (e.g. Computers; smartphones)
- Speed of access to sharing of data and images

Global Reach

- Criminal law has been built around jurisdictional boundaries
- Offenders have a reach to victims in a geographically unlimited environment
- Over 50% of cybercrimes are transnational

Absence of a capable guardians

- Surveillance is difficult
- Jurisdictional cooperation is needed - this takes time and resources
- Extradition agreements
- Expansion of guardianship - particularly, self-protection of victims

Shift in Cybercrime Targets

- Dramatic shift in cybercrime targeting, as criminals move away from individual consumers and focus instead on enterprise opportunities
- Recent breaches at large data warehouses have resulted in the theft of hundreds of millions of pieces of Personality Identifiable Information (PII). PII is a valuable commodity.

Organised Crime in Cybercrime

A most disturbing development is that highly organised crime syndicates are playing a leading role in the explosion of cybercrime. According to FBI, these organisations operate with specialists in each area of expertise.

Organised Crime in Cybercrime

- *Organisation Leaders* assemble the team and choose targets
- *Coders* write the exploits and malware
- *Distributers* trade and sell stolen data

- *Tech Experts* maintain the criminal enterprise's IT infrastructure
- *Hackers* search for and exploit vulnerabilities in applications, systems and networks
- *Fraudsters* woo potential victims with social engineering schemes like phishing and spam
- *Hosted System Providers* offer illicit content servers
- *Cashiers* control drop accounts and provide names and accounts to other criminals for a fee
- *Money Mules* complete wire transfers between bank accounts
- *Tellers* who transfer and launder illicit earnings through digital currency services

New or Old Crimes? What is Cybercrime?
Is cybercrime an entirely new form of offending? Is it simply old crimes committed in new ways?
Is it BOTH - however, majority are existing crimes committed in new ways

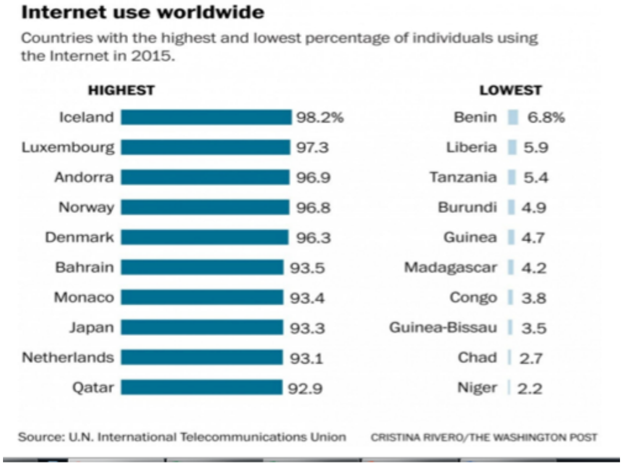
The Case of Identity Theft - Provide a modus operandi for both types of offenders - traditional? Cyber enabled?

Week 2: Scale and Impact of Fraud and Cybercrime

Online Engagement - How connected are we?

Percentage of individuals using the internet

- Europe = 79.1%
- The Americas = 65%
- Asia and the Pacific = 41.9%



Source: U.N. International Telecommunications Union CRISTINA RIVERO/THE WASHINGTON POST

UK Experience

In January 2017, the Crime Survey for England and Wales included cybercrime offences for the first in it its annual report.

There were an estimated 3.6 million cases of fraud and 2 million computer misuse offences in a year; more than two thirds were specifically labelled as being examples of cyber crime. This means they involved the internet or online activity. c

Top Fraud and Online Crime:

- Bank Account Fraud
- Phishing (2.4M)

"In the past, burglary and theft of vehicles were the high volume crimes driving trends but their numbers have fallen substantially since then. When the crime survey started (35 years ago), fraud was not considered a significant threat and the internet had yet to be invented. Today's figures demonstrate how crime has changed, with fraud now the most commonly experienced offence."

UK government announced it was investing 1.9 billion pounds in cybersecurity over five years.

The National Cyber Security Strategy is to be used to develop a strategy for tackling hackers and the problems they pose to national security as well as to the public individually

Collecting Data - UK

<u>NFIB</u>

- The National Fraud Intelligence Bureau (NFIB) sits alongside Action Fraud within the City of London Police which is the national policing lead for fraud.
- The NFIB takes all Action Fraud report and uses millions of reports of fraud and cybercrime to identify serial offenders, organised crime gangs and established as well as emerging crime types.

<u>Action Fraud</u>

- Action Fraud is the UK's national reporting centre for fraud and cyber crime where you should report fraud if you have been scammed, defrauded or experienced internet crime.

- The service is run by the City of London Police

US Experience

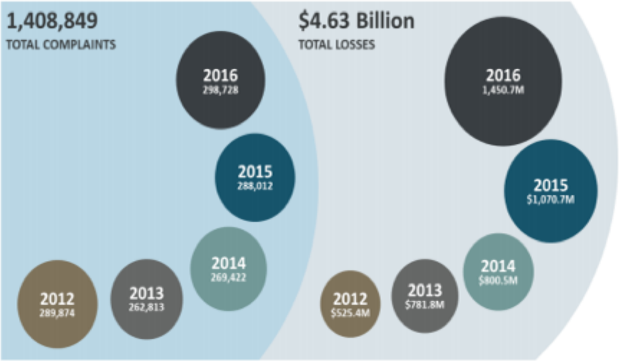
In 2016, US introduced the Cybersecurity National Action Plan

- The FBI is the lead federal agency for investigating cyber attacks by criminals, overseas adversaries, and terrorists
- The Department of Justice, acting through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF), takes the lead on threat response activities;
- The Department of Homeland Security, acting through the National Cybersecurity and Communications Integration Centre, leads asset response activities;
- The Office of the Director of National Intelligence, through its Cyber Threat Intelligence Integration Centre, leads intelligence support and related activities.

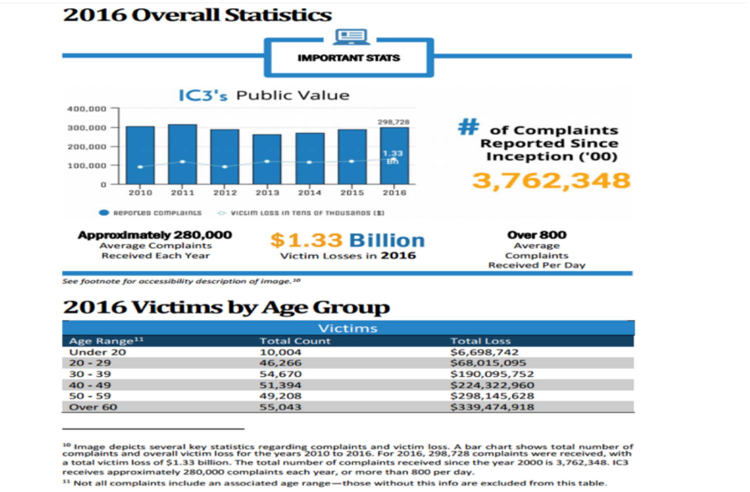
The Internet Crime Complaint Centre (IC3), established in 2000

- The mission of the IC3 is to provide the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected Internet-facilitated fraud schemes and to develop effective alliances with law enforcement and industry partners
- Information is analysed and disseminated for investigative and intelligene purposes to law enforcement and for public awareness
- In 2016, IC3 received a total of 298,728 complaints with reported losses in excess of $1.3billion
- This past year, the top three crime types reported by victims were non-payment and non-delivery, personal data breach, and payment scams
- The top three crime types by reported loss were BEC, romance and confidence fraud, and non payment and non-delivery scams.

Publishing Statistics



Only an estimated 15% of the nation's fraud victims report their crimes to law enforcement.



2016 Overall Statistics

IMPORTANT STATS

IC3's Public Value
400,000
300,000
200,000
100,000
0
298,728
1.33 Bn
2010
2011
2012
2013
2014
2015
2016
Reported complaints
Victim loss in tens of thousands ($)

# of Complaints Reported Since Inception ('00)

3,762,348

Approximately 280,000
Average Complaints
Received Each Year

$1.33 Billion
Victim Losses in 2016

Over 800
Average
Complaints
Received Per Day

See footnote for accessibility description of image.[10]

2016 Victims by Age Group

Victims		
Age Range[11]	Total Count	Total Loss
Under 20	10,004	$6,698,742
20 - 29	46,266	$68,015,095
30 - 39	54,670	$190,095,752
40 - 49	51,394	$224,322,960
50 - 59	49,208	$298,145,628
Over 60	55,043	$339,474,918

[10] Image depicts several key statistics regarding complaints and victim loss. A bar chart shows total number of complaints and overall victim loss for the years 2010 to 2016. For 2016, 298,728 complaints were received, with a total victim loss of $1.33 billion. The total number of complaints received since the year 2000 is 3,762,348. IC3 receives approximately 280,000 complaints each year, or more than 800 per day.

[11] Not all complaints include an associated age range—those without this info are excluded from this table.