Abstracts

Listed in alphabetical order by title

Technology stream

Android Mobile Forensics for Files System

Aiman Abdul-Razzak Fatehi Al-Sabaawi and Ernest Foo, Science and Engineering Faculty, Queensland University of Technology

This presentation gives a comprehensive overview of forensic analysis of Android phones and discusses the fundamentals of acquiring and analysing an Android disk image. The challenges of Android forensics include the complexity of the Android operating system, the variety of procedures and tools for obtaining data and difficulties with hardware set-up. Expensive commercial tools for acquiring logical data can fail.

A new open source technique can solve these challenges and recover Android data with high accuracy and integrity. Manual, logical and physical acquisition techniques are used to retrieve data from a Samsung Android 4.2.2. Four tools are used to analyse recovered data. Analysis shows that the technique can retrieve contacts, photos, videos, the call log and SMS messages.

Artificial intelligence and robotics in 2030s social technologies: A possible scenario and the challenges to society

Laurie Lau, Asia Pacific Association of Technology and Society, Hong Kong

Artificial Intelligence (AI), including robotics, is different to traditional coding in many ways. Self-learning coding systems based on artificial intelligence can make decisions and modify their instructions autonomously and can be controlled by humans only to a limited extent. Such systems entering the commercial marketplace pose a big challenge to public governance, law and policing more broadly. It is difficult to ascertain whether any natural human could be held liable for the actions of AI systems or for any harm done to society. Against that backdrop, this presentation will discuss whether current governance, law, policing and social controls on the internet apply to AI systems or whether we need to invent new rules for them.

Bring your own awareness through practising educational mobile gaming

Khulood Al Zaabi, American University in the Emirates

Mobile learning is evolving due to the development of mobile computing and the rapidly rising use of mobile technology around the globe. Therefore, elementary mobile awareness and education about cybersecurity is needed. In this context, a digital game is an entertaining way of educating mobile users and persuading them to enhance their privacy protection.

The purpose of this presentation is twofold: first, to discuss how wary people are about mobile computing risks and, second, to introduce a novel mobile app called EduCyberAware, which increases cybersecurity awareness. The app was developed based on the results of a survey of people of different genders, ages and levels of education. It teaches users to enhance their security, addressing areas of concern identified in the survey. This research showcases that not everyone is adequately aware of the risks associated with technology use. Furthermore, the survey revealed that even professionals had been victims of cyber attack. Based on the survey results, it is recommended that federal security organisations educate mobile users through digital games.

Cyberthreat intelligence information sharing

Edilson Arenas, Central Queensland University

The sociopolitical and technological transformation of mankind is currently being challenged by a series of sophisticated cybersecurity threats and technology-enabled crimes. Governments, academics, industry groups and business organisations are currently engaged in joint efforts to find cost-effective ways of detecting and protecting against this malpractice. Unfortunately, a number of factors have hindered the success of these efforts, with the sharing of clean data and cyber intelligence at the top of that list. Sensitive legal, ethical and business issues make it difficult to share cybersecurity information and find reliable data for research, development and testing.

This presentation argues that to address this problem we need a global collaborative effort to standardise the sharing and structure of cyber intelligence. Such standardisation will ultimately lead to the development of innovative strategies and a greater ability to create strong, reliable and efficient layers of security. The presentation outlines a new approach to cyber intelligence information exchange based on several current research frameworks.

Deep sea phishing: malicious URLs detection using deep learning

Mamoun Alazab, Macquarie University
MingJian Tang and Jeremy Lee, University of New South Wales

Malicious spam emails increasingly contain URLs to compromise the security of a computer. These malicious emails try to disguise their content to avoid anti-virus scanners. Malicious URLs embedded in emails add another layer of disguise, where the email content tries to entice the recipient to click on a URL that links to a malicious website that will cause the computer to download malware—known as 'drive-by download'.

Recent literature studies revealed that the number of observed spear phishing attacks doubled in 2016, while the average number of spear phishing attacks detected fell sharply. The review also indicated the shortcomings of current reactive detection techniques, which largely rely on checking URLs against a blacklist. This method is only successful against known URLs, not new ones. Given the ever-changing tactics adopted by cybercriminals, such as using URL-shortener links, landing pages and new URLs, the blacklist approach can fail.

This preliminary research investigates the usefulness of applying an advanced artificial intelligence technique known as deep learning for this purpose. The research analyses malicious top-level domains using a deep learning model to improve detection of malicious URLs, using a real data set of more than 30,000 malicious URLs. This work shows it is possible to reduce reliance on feature extraction and URL blacklists, which often do not update as quickly as the malicious content they attempt to identify. Such methods could reduce the number of resources needed to identify malicious URLs. The research will provide the basis for further development of cybercrime prevention strategies.

Development of ICS Honeynet for cyber tagout in critical Infrastructure

Shoya Kojima, Tomomi Aoyama, Ichiro Koshijima, Shingo Abe and Yuma Takayama, Nagoya Institute of Technology, Japan

Cyber attacks targeting critical infrastructure have been increasing with the significant advance in technology. In fact, cyber attacks against power grid substations in Ukraine caused a large-scale blackout in 2015, affecting 1.4 million people. In following year, the attack was repeated. Therefore, a resilient industrial control system (ICS) is needed so that the infrastructure can continue operating safely even if the network is attacked.

In this presentation, the authors discuss a cybernetic system which isolates attacked ICS devices and misleads attackers, directing them to a designated fake network. The fake network includes real and virtual devices and is called Honeynet. The purpose of the system is to manipulate the attacker and isolate the invaded area to gather information about the attacker from the affected devices.

Identity, blockchain and cybercrime

Greg Adamson, University of Melbourne

By design, both the internet and the World Wide Web have no requirement or capacity to identify participants. As a famous *New Yorker* cartoon put it, ‘On the internet, no one knows you’re a dog.’ Many approaches to identity management on the internet have sought to make up for this deficiency, with mixed success. Identity is not a challenge that can be simply solved, in part because issues of privacy and human dignity prevent a simple categorisation and labelling of everyone.

The enormous growth of the Internet of Things has transformed a significant problem into an existential threat: the possibility of tens of billions of devices with poor security, no patch management and little owner awareness being used as bot armies to launch massive distributed denial-of-service attacks is not a comforting thought for this growing industry.

While security is in general an add-on for the internet, one security technology, Satoshi Nakamoto’s blockchain, uses the inherent characteristics of the internet (action by distributed and cooperating but not trusting or known parties) to provide confidence in distributed ledgers.

This presentation describes research at the intersection of identity and agency, blockchain and security vulnerabilities such as with the Internet of Things. Activity at this point of intersection is currently part of the discussion about governance and standards for blockchain taking place in many standards bodies including IEEE, W3C, Hyperledger and ISO.

Integrating “self-efficacy” into a gamified approach to thwart phishing attacks

Nalin Asanka Gamagedara Arachchilage, Australian Centre for Cyber Security, School of Engineering and Information Technology, University of New South Wales, Australian Defence Force Academy

A cyberthreat which is particularly dangerous to computer users is phishing. Phishing is better known as online identity theft, where a cybercriminal attempts to steal sensitive information from a victim such as user names, passwords and online banking details. Automated anti-phishing browser plug-in tools are used to alert users to potentially fraudulent emails and websites. However, these tools are not completely reliable in detecting and protecting people from phishing attacks, because humans are the weakest link in information security. It is impossible to completely circumvent the end user.

In personal computer use, therefore, educating the end user is essential. Educational researchers and industry experts agree that well-designed security education can be effective. However, the question of how best to design security education for the end user is discussed much less.

Therefore, this presentation focuses on an innovative game that educates people about phishing attacks. One of the main reasons phishing scams succeed is a lack of user knowledge. Therefore, this research investigates the elements that influence behaviour to create an educational game that will enhance people’s ability to avoid phishing scams.

Integrity orientated clustering of IoT system

Hideyuki Shintani, Tomomi Aoyama, Ichiro Koshijima, Shingo Abe and Yuma Takayama, Nagoya Institute of Technology, Japan

In recent years, there has been a trend in various industries towards using the Internet of Things (IoT) and cyber physical systems. However, IoT devices are highly vulnerable to cybercrime. For example, it has been found that there are over 22,000 web cameras vulnerable to attack just in Barcelona. Cybercriminals can take down servers and websites by exploiting hundreds or thousands of vulnerable devices and building botnets. Infected devices can also be used to infect other devices, incorporating them into the botnet.

Usually, each IoT device in a system independently acquires data on its position, and a cloud system integrates sensory data to analyse the overall situation of the local IoT devices. However, when the sensor cannot acquire adequate data due to device failures or cyber attacks, abnormalities in the configuration become difficult to detect. In this research, the authors propose a resilient IoT system structure which can detect threats.

Localisation of automobiles in urban environment using machine intelligence techniques for prevention of car hacking and cybercrime

Ashwani Kumar, Electrical and Instrumentation Engineering Department, Sant Longowal Institute of Engineering and Technology, Longowal, India

Identifying the location of vehicles is challenging but useful in preventing car hacking and cybercrime. For an autonomous vehicle to navigate in a known or unknown environment, it needs to know its current position. Many 2D and 3D based methods using techniques from computer science, artificial intelligence and machine learning are being employed for the task. These methods allow a car to navigate in a simple environment. However, in the presence of hurdles, poor illumination, occlusions and unexpected scene changes, existing methods either fail or perform badly. For an autonomous vehicle to navigate in such tough conditions, an image based method using a database of environmental features is needed. A fast and efficient query image detection system can extract the current location of the car within the environment. It helps the automobile to navigate and avoid collisions.

Malware in the Western Australian Government

Peter Bouhlas, Office of the Auditor General, Western Australia

Industry experts agree it is a case of not if but when you will be attacked. Government agencies that store significant amounts of confidential and highly desirable personal information are prime targets for infiltration and attack. The cost to the Australian economy of responding to cybercrime, including malware, is estimated to be as high as $1 billion per year.

An audit carried out by the Office of the Auditor General (OAG) found all six agency networks investigated had experienced numerous attacks and malware downloads. The audit sought to determine whether the selected government agencies had effective controls to prevent, detect and respond to malware threats and malicious software infecting their computer systems.

This presentation will discuss how the OAG tested six agencies to assess whether IT security was effective at countering malware threats. The audit analysed agency network traffic for any evidence of active malware infections or attempted malware attacks. It also compared security processes and tools against recommended practice.

All agencies experienced attacks that were able to defeat at least one security control or technology. The control failures identified during this audit were consistent with the findings of the OAG's annual Information Systems Audit Reports. The findings illustrated yet again the importance agencies should place on ensuring that often basic, easily implemented controls are in place and operating effectively. But the evolving malware threat also requires agencies to constantly improve their security processes and upgrade to more advanced security tools to further secure their networks.

Profiling security and privacy threats for smart home IoT devices

Hassan Habibi Gharakheili and Vijay Sivaraman, Electrical Engineering and Telecommunications, University of New South Wales, Sydney
Narelle Clark, Australian Communications Consumer Action Network (ACCAN)

The internet continues to give us the opportunity to enjoy incredible experiences, be entertained and informed, and keep in contact with others across the street or the globe. Internet connected devices offer us unparalleled freedom and flexibility. These devices are also becoming more important for our sense of personal safety and security. This Internet of Things (IoT) includes televisions, webcams, smoke alarms, fitness trackers, climate control systems and even smart light bulbs. Experts predict that consumers across the world will use more than 10 billion IoT devices by 2020.

However, IoT devices are susceptible to attack. Many internet connected devices have poor security measures that make them vulnerable, and these have the potential to reveal private data and information that may further hurt or expose us. A typical smart home equipped with multiple devices is at significant risk of cyber attack. This vulnerability compromises our personal data and threatens our personal safety.

A test of 20 IoT devices found that five do not encrypt data, making it easy for intruders to intercept user information. Four of the devices allowed attackers to manipulate them so they could execute remote commands, and two of the webcams tested had weak passwords, making them easy to hack. More than half the devices tested could be rendered dysfunctional if bombarded with a high volume of traffic and most could be manipulated to launch attacks on other devices.

Several options to manage the risks of IoT attack need to be considered, ranging from consumer education to legislation. Perhaps it is also time to adopt a star-rating system to give consumers greater information about the security of their IoT devices.

Recurrent Neural Network (RNN) base computational model for cyberattack detection

Teik-Toe Teoh, Centre for Research in Cyber Security, Singapore University of Technology and Design, Singapore
Yok-Yen Nguwi, School of Business (IT), James Cook University, Singapore
Yuval Elovici and Wai-Loong Ng, ST Electronics (Info-Security) Pte Ltd, Singapore

A recurrent neural network (RNN) is a form of neural network which contains an internal state with the ability to store temporal information. This property makes RNN a good choice for handling large and sequential cybersecurity data. Each neuron in RNN has a time-varying activation. This study collected three days of data that built up to 36 million log files (approximately 36 gigabytes). That total included 47 instances of malware.

Network traffic data comes in at very high speed, resulting in large files being generated, so batch processing was used to process the data. This study examined RNN architecture to detect cybersecurity threats. The RNN algorithm classifies the long sequence of data into three categories: cybersecurity attack, unsure, and no attack. It is a deep learning model that works for long series of data. The initial error rate was 6.55 per cent, but that rate was subsequently reduced to 0.35 per cent after training the model with 10,000 iterations. The training and testing time is about five seconds.

Text Thermal Alert Model: an analysis of Twitter lingo for privacy leaks and tweet regrets

R Geetha and S Karthika, SSN College of Engineering, Tamil Nadu, India

The micro-blogging website Twitter allows users to post thoughts, or 'tweets', of up to 140 characters. As tweets are available to the public, caution is needed when posting personal or incriminating information. To minimise privacy breaches, an intelligent system identifies 53 critical keywords in tweets such as 'credit card', 'my photo', 'investment', and 'phone number' and calculates vulnerability by analysing privacy measures like universality and confidentiality.

This system is demonstrated in a simulated social network with agents that acquire behavioural properties from real Twitter users. Whenever a user tweets, the content is analysed using several machine learning algorithms and the user is alerted if the message contains personal information. Additionally, the level of private information disclosed in a particular tweet is indicated with a colour ranging from green (highly secure) to red (highly insecure), encouraging the user not to post the message or to rephrase it. This system will assist Twitter users by analysing the community they most frequently interact with and predicting the vulnerability of their tweets.

Research and policy stream

A research study concerning applicability of law on cyberbullying among law students: the case of Indonesia

Antonius Wibowo, Atma Jaya Catholic University of Indonesia

According to Indonesian law, a victim of cyberbullying can report the crime to police or to the Ministry of Communication and Information, who generally then prosecute it. Under Indonesia's laws, victims of crime also have the right to compensation, restitution and assistance.

This presentation analyses knowledge of the law on cyberbullying based on Bloom's theory of taxonomy (named after Benjamin S Bloom). According to this theory, cognitive learning has six hierarchical levels of complexity: knowledge, comprehension, application, analysis, synthesis and evaluation. Someone can apply what they have learnt if they have sufficient knowledge and comprehension.

This research used a survey with a mix of closed and open-ended questions to investigate knowledge of the law on cyberbullying among law students at Atma Jaya Catholic University. The findings indicate most students have little knowledge of the law and no comprehension of the procedures for reporting cyberbullying or claiming compensation.

Australian police and cybercrime

Rick Sarre, University of South Australia

Australian police regularly assert that they have, as part of their mission, a key place in the fight against cybercrime. Given the many other calls upon their resources, to what extent is this true? What role should they have? Are there steps that can be taken to increase their presence in this field, or should the work be handed over to specialist agencies only?

Behind the screen: Online child exploitation in Australia

Indika Chandrasekera and Elizabeth Sheridan, Anti-Slavery Australia, University of Technology Sydney, New South Wales

This presentation will reveal the key findings and recommendations of Anti-Slavery Australia's report *Behind the screen: Online child exploitation in Australia*. *Behind the screen* is the first report of its kind in Australia, examining international and domestic responses to online child exploitation. It reviews data previously unavailable to the public, provides expert commentary drawn from interviews with representatives of leading law enforcement agencies, and delivers a comprehensive summary of Australia's response to online child exploitation.

The report outlines the relationship between state, territory and Commonwealth criminal legislation. This research uncovers significant barriers to understanding and responding to online child exploitation in Australia, including a lack of comprehensive national crime data, and inconsistencies in legislation between jurisdictions.

The report incorporates preliminary research on sentencing trends for Australian offenders, who are both viewers and distributors of online child exploitation material. The report finds that there is a substantial need for sentencing to reflect the seriousness of these offences, especially in the context of increasingly explicit and violent depictions of child abuse. The research also explores the efficacy of Commonwealth legislation in addressing the prominent role Australian administrators of online child exploitation networks have in driving the production of content.

Behind the screen examines barriers to the detection and prosecution of offenders and the identification of victims—particularly the darknet—as well as the role of internet service providers. The presentation will outline recommendations to strengthen Australia's response to online child exploitation.

Characteristics of cybercrimes: evidence from Chinese judgement documents

Tianji Cai, Department of Sociology, University of Macau, China

China has witnessed a rapid growth in the number of internet users as well as an unprecedented increase in cybercrime. Although many studies have suggested the growth in cybercrime may be related to the widespread use of the internet for entertainment, the low average income of internet users, the high level of skills among users and their employment structures, studies on actual offenders are rare.

Taking advantage of newly released judgement documents, this presentation examines the basic characteristics of cybercrime offenders in China. It analyses 2,075 judgement documents which cover information-related, computer-related, content-related and copyright-related offences. There is a specific focus on the connections between offenders and the underground economy. This study will not only help researchers to gain a better understanding of cybercrime but also benefit those in the wider community attempting to apply text-mining techniques to social science research.

Cybercrime: Awareness and mitigation policies in Ghana

Kolog Solomon Polpiem and Sidique Gawusu,
Nanjing University of Science and Technology, Nanjing City, China
Nathaniel Gyamfi Kontoh, Hohai University, Nanjing City, China

Cybercrime is an area of no small concern in the virtual world. More and more criminals are exploiting the speed, ease and anonymity of the internet to commit an increasing variety of criminal deeds that know neither physical nor virtual borders, causing serious harm and posing very real threats to victims worldwide. This is of great significance in Ghana, where the increase in internet use has been unprecedented. As individuals and companies rush to get access to the internet, the issues related to cybercrime are gaining urgency with equal speed. With few well-protected networks in this new territory, cybercriminals have found a new home base.

This presentation focuses on the development of cybersecurity policies in Ghana. It also looks at the rate at which cybercrimes are reported. This research collected data through case studies, questionnaires and face-to-face interviews with individuals, private corporations and other stakeholders in Ghana. The core objective was to discover to what extent citizens of Ghana have been victims of cybercrimes. The responses revealed a significant finding. Based on this investigation, this presentation makes recommendations that could help battle cybercrime in Ghana.

Cybercrime and cybersecurity in ASEAN

Lennon YC Chang, School of Social Sciences, Monash University, Victoria

This presentation examines the trends in and challenges of cybercrime in the Association of Southeast Asian Nations (ASEAN) region. The ASEAN region is an emerging cybercrime market for which there is limited research. What are the trends in and challenges of cybercrime in ASEAN? Are current conventions appropriate for ASEAN? What are the challenges faced by ASEAN countries when collaborating internationally against cybercrime? This presentation aims to answer these questions and to consider whether the strategies to combat cybercrime developed in the global north are relevant to ASEAN. This research provides an overview of cybercrime trends in the ASEAN region, assesses current measures adopted by ASEAN countries to combat cybercrime, and makes policy recommendations to strengthen those measures.

Cyberterrorism: a review of risks

Professor Rod Broadhurst, Australian National University

The exploitation of the Internet in the furtherance of violent extremism and the capitalising on its many advantages by criminal actors of every stripe has unsurprisingly emerged as a pressing policy challenge for many governments. Extremist violence seeks to undermine the legitimacy of the state by performing acts of terror that mock the traditional monopoly of violence associated with state authority. Finding the balance between a secure yet open Internet is a work in progress. The potential chilling effects of (excessive) securitisation of cyber space on the creative uses and benefits of the shared knowledge bounty provided by widely used open online resources such as Wikipedia (notably WikiProject Medicine), require an approach that steers regulatory responses and countermeasures carefully past unintended consequences. The incremental steps already taken to better secure the benefits of the new communication technologies at the international (mutual legal assistance), national (holistic cybersecurity strategies) and civic/ individual (community policing, and education) levels provide valuable lessons about how to reduce the impacts of cyber-terrorism, terrorism and cybercrime in general.

From the cyber to the 3D printer: Darknet design files and 3D printed firearms

Dr Monique Mann, School of Justice, Queensland University of Technology
Dr Angela Daly, School of Law, Queensland University of Technology

Following the 1996 Port Arthur massacre, the Australian government introduced legislation to restrict the import, sale and licensing of firearms, which was largely successful in reducing gun-related crime. However, Australia's gun control laws have been outpaced by new technologies. With design files for a functional gun now available on the darknet and other file-sharing sites, anyone with an internet connection and a cheap 3D printer can manufacture illegal weapons. There is emerging evidence of 3D printed gun parts being found by police.

As is often the case with new technologies that can be used for nefarious purposes, the legal system and police have been largely reactive, with the exception of specific offences related to 3D printed guns and their design files introduced in New South Wales in 2015. Moreover, there has been limited legal and criminological research into this phenomenon and the wider implications of 3D printed firearms.

This presentation aims to fill this gap through an examination of 3D printing and crime, setting forth an agenda for further research on this topic in Australia and internationally. The presentation will explain the technology of 3D printing, discuss the relationship between 3D printing and cybercrime, including darknet and file-sharing sites, and conclude with consideration of some of the legal and policing implications for new technologies such as 3D printing.

Identity theft and mobile phone portability: A failure of regulatory responses

Dr Terry Goldsworthy, Bond University, Queensland

In Australia identity crime now costs some $2.6 billion per year.
Part of this expansion of technology-enabled crime is the phenomenon of criminals engaging in unauthorised porting of a victim's phone, an activity that is becoming increasingly common.

Mobile phone number portability was introduced in 2001 as a government-mandated requirement for telecommunication providers. The portability of mobile phone numbers has now been targeted by criminal elements as a way of stealing the identity of victims and using the control of the phone as a means of committing further offences. Much of our financial and lifestyle information is now contained on our mobile phones.

This presentation will address the expanding notion of identity and the effect technology has had on traditional criminal enterprise. It will rely on data from the United States and Australia to show that this type of offence is an emerging opportunity for criminal entrepreneurs. The presentation will also examine the modus operandi of this type of offence and outcomes for victims.

The discussion will analyse the policy and regulatory responses to phone porting and the failure to aggressively tackle this issue. The increased use of smart phones and the expanding criminal market for this type of offence has created significant challenges for law enforcement. The researchers will argue that customer convenience is being prioritised over security and crime prevention responses.

Information technologies and fraud risks for the Commonwealth

Penelope Jorna, Australian Institute of Criminology

Information and communication technologies (ICT) can be the target of criminal activity as well as a tool used to commit criminal acts. In the 2016–17 financial year Commonwealth spending on information technology systems and infrastructure for public service entities totalled almost $10 billion. Fraud risks for organisations are high when new ICT is being rolled out, and this risk is further increased when the organisation has access to large amounts of money. These factors make the Commonwealth a particularly attractive target for fraud.

Fraud in the public sector can be perpetrated by public servants, who may abuse their privileges for personal gain (internal fraud), or perpetrated by individuals external to the entity (external fraud). It is likely that many instances of the misuse of ICT go undetected and unreported. Fraud in general is known to be vastly underreported, and fraud involving ICT may be particularly so.

This presentation examines the fraud risks faced by Commonwealth entities with the increased reliance on technology. It also discusses the preventative factors employed by organisations such as fraud control plans, policies and technical standards for data security to minimise the risk of ICT misuse. It identifies intervention points at which prevention and detection methods may be focused. Findings from the Australian Institute of Criminology's *Fraud against the Commonwealth* reports are used to assess the nature of external and internal fraud cases in Commonwealth entities and how fraudsters may adapt their behaviour to changing technologies.

Investigation of cybersecurity practices in academic institutions

Anurag Jain, Swati Maurya, Sanur Sharma and Ajeet Singh,
University School of Information, Communication and Technology
Guru Gobind Singh Indraprastha University, Delhi, India

Cybersecurity is one of the most important aspects of today's information systems, and linking it with the education system is essential. There has been a recent rise in cybersecurity attacks in education systems, as these systems are vulnerable to breaches. This presentation focuses on the cybersecurity challenges that exist in educational institutions and how to curb them. While academic institutions have adopted various measures to achieve compliance with the current security standards, these measures have had limited success in influencing user behaviour. Keeping this in mind, this research focuses on the threats and vulnerabilities in the education system and the security guidelines that can be adopted to overcome them.

Measuring information security readiness in a distributed cloud environment

Champake Mendis, Charles Sturt University, New South Wales,
Triple A Super, Victoria
Roshan Dhakal and Rafiqul Islam, Charles Sturt University,
New South Wales

In a highly competitive business environment, analytics is essential in gaining an advantage. Customers who are mainly retirees yearning to maximise their income after retirement select self-managed super fund (SMSF) administrators who can provide a good return on investment for a nominal cost.

With the advent of cloud computing, organisational overheads are reduced, with lower administrative costs, lower staff requirements and cloud bound applications which are easier to deploy. Cloud computing offers pay-as-you-go costs and other features such as simplicity and expandability. The cloud is an ideal platform for complicated calculations, scientific simulations and complex business analytics, which may need large amounts of computational resources such as processing speeds and storage capacity.

Education, training and awareness is the bottom line in preventing an organisation from suffering information security catastrophes caused by human factors. This presentation offers a way of reducing organisational risks and threats to an acceptable level. This research investigates how to measure the effectiveness of information security education, training and awareness programs in an organisation. The research also aims to develop metrics to assess the information security readiness of an organisation.

Not just 'revenge': The nature and correlates of image-based sexual abuse perpetration by Australian adults

Dr Anastasia Powell and Dr Nicola Henry, RMIT University, Victoria
Dr Asher Flynn, Monash University, Victoria

'Revenge pornography' is a media-generated term referring to the distribution of nude, sexual or sexually explicit images without the depicted person's consent, often via social media or mobile phones. Yet the term itself is misleading, as not all perpetrators are motivated by revenge, and not all images can be described as pornography. The term may also be offensive to many victims, as it can minimise the harms they experienced when a nude or sexual image was created and/or distributed without their consent. This is partly why academics and government agencies are increasingly using the alternative terms 'image-based abuse' or 'image-based sexual abuse'.

Image-based sexual abuse is increasingly being criminalised in Australian states and territories, as well as in many jurisdictions internationally. As such it represents an important and rapidly developing cybercrime issue. This presentation discusses the findings of the first national online survey of over 4,000 Australian adults about image-based sexual abuse perpetration. Implications of this research for policy and practice in response to image-based abuse in Australia are then discussed, along with directions for future research in this rapidly emerging field. This project has been undertaken with funding from the Criminology Research Council (CRG 08/15-16).

Situations of cybercrime and the corresponding social responses in modern China: Learning from Western experiences

Hua Zhong, Chinese University of Hong Kong

Social scientists have long been concerned about the impact of modernisation on social behaviour. In recent decades, scholars have observed that new types of crime, especially online offences, are increasing along with the prevalence of advanced technology. Cybercrime then draws substantial attention from multiple disciplines, and various empirical studies have been conducted in the West to examine the causes and social impacts of cybercrime. Although this area has become increasingly important in the world, very few social science researchers in mainland China have paid attention to it.

Based on 56 cybercrime cases reported by two major Chinese media organisations in the last three years, this study aims to provide preliminary typologies of cybercrime in modern China and the corresponding social responses. The research has identified the rising prevalence of three major types of cybercrime: communications in furtherance of criminal conspiracies such as drug trafficking, gambling or sexual offences; dissemination of offensive material such as sexually explicit materials in mainland China; and sales or investment fraud using digital technology.

The legal definitions of and punishments for cybercrime in the Chinese context are mainly learnt from the West. The criminal justice system in China faces similar challenges to Western societies when dealing with cybercrime cases—for example, the globalisation of criminal networks and the fact that law enforcement technology lags behind that of criminals.

However, the social responses to different types of cybercrime in China are quite diverse and show great disparities compared to the Western experience. For example, the Chinese people are more tolerant of privacy-related cybercrime and more sensitive about online fraud. According to social constructionist theory, opportunity theory and Merton's anomie theory, such social responses are partially due to political propaganda, the prevalence of internet use in both rural and urban areas, and the anomic situations in modern China (low levels of belief in the rule of law and strong motivations for financial success).

Specialist police cybercrime units: What is best practice for fighting cybercrime?

Dr Diarmaid Harkin and Associate Professor Chad Whelan, Deakin University, Victoria
Dr Lennon Chang, Monash University, Victoria

Cybercrime is an escalating priority for police and security agencies at national and international levels. As a result, the role played by specialist cybercrime units at the state level is increasing in importance. This presentation reports on original empirical research conducted with Victoria Police's E-Crime Squad and the New South Wales Police Force's Fraud and Cybercrime Squad using a mixed methods approach of survey data and interviews. Initial data and findings will be presented on the challenges currently faced by specialist cybercrime units. International research has identified resourcing, training, skills, IT expertise and partnerships both internal and external as common struggles for specialist police units. This presentation will examine the Australian experience vis-à-vis similar international units and will also provide an initial assessment as to how state-based police organisations can better equip themselves with the knowledge and skills required to navigate the evolving challenge of cybercrime.

The dangers to data protection insider triggered—an empirical study

Subashree Anantaraman and Dr Ravi N Thodla, Faculty of Management, SRM University, Chennai, India

Gathering, storing and analysing information has shifted from being a manual process to a technology assisted one, and this has brought savings in time and resources. At the same time, it has created challenges, with more and more immoral use of otherwise sound advancements in information technology. The consequent threat of security breaches has emerged as one of the most dangerous challenges facing governments and enterprises alike.

It is sometimes said that progress is the exchange of one form of nuisance for another, but that does not stop us from seeking progress. This presentation examines the need to invent and fine-tune sophisticated models that mitigate the risk of security breaches and weed out malicious attempts to compromise security.

The double-edged sword of identity misuse in cyberspace

Dr Russell G Smith, Australian Institute of Criminology

Criminal misuse of personal information is not new but has become one of the most prevalent criminal activities in recent times, affecting individuals, businesses and government agencies alike. It is estimated that identity crime affects hundreds of thousands of Australians each year and comparable numbers in other developed nations. People in developed nations are most often targeted by criminals, who are often located in less well developed countries.

This presentation examines the nature and extent of identity misuse and considers the extent to which cyberspace has contributed to the problem by acting as a medium for obtaining personal information, disseminating dishonest invitations and persuading victims to provide valuable information and funds. It concludes by considering how cyberspace can also be a solution to the problem, by providing advice on how to avoid victimisation, by enabling illegal communications to be tracked, and by providing secure, alternative means of identification and authentication of identity information.

Cyberspace is the quintessential double-edged sword. The solution to the misuse of personal information in cyberspace lies in collaboration among those who create and manage digital technologies, those who monitor vulnerabilities and security weaknesses, and those who design policy and practical strategies to prevent misuse.

The future of intellectual property in a world of artificial intelligence and robotics

Professor Hedi Nasheri, Kent State University, United States of America

Artificial intelligence (AI) has been generating inventive output for decades, and the continued and exponential growth in computing power is now poised to take creative machines from novelties to major drivers of economic growth. For example, in today's financial marketplace smart machines powered by complex algorithms run much of finance. Financial tasks that previously required human teams to exert hours, days or weeks of effort are now being done by artificial intelligence, algorithmic models and supercomputers that perform those tasks exponentially faster and cheaper. High-frequency trading programs powered by artificial intelligence trade billions of dollars in securities and commodities across the world in fractions of a second without any human assistance, in public markets as well as in private dark pools. Autonomous supercomputers assist financial institutions in assessing risk and managing assets.

An innovation revolution is on the horizon, and this phenomenon poses new challenges for policymakers and legislative bodies globally. In the United States, the US Patent Office and Congress need to reconsider the boundaries of intellectual property rights and protections. Companies like Google, Facebook and Blockstream have announced that they are developing technology in the open in areas like artificial intelligence, engaging in massive sharing of what would otherwise be proprietary technology—not because of altruism but because of the benefits of open innovation to recruitment, culture and speed.

Artificial intelligence poses a major threat to companies' intellectual property and the risks cannot be ignored. Existing laws are insufficient to protect against the unique threats posed by AI. Now is the time to call for legislative action and regulation. It is important for policymakers to seriously consider the social concerns surrounding the robotics revolution and enact safeguards that minimise the risks associated with using, selling, transferring and programming AI.

The future of information security in the digital economy

Ivano Bongiovanni, Paula Dootson, Queensland University of Technology

The challenges of information security lie at the intersection of different domains in the digital economy, with significant impacts for individuals, organisations and governments: the use of digital technologies, the diffusion of deviant online behaviours, the unprecedented reliance of modern companies on IT systems, the rise of the 'economy of people' over the 'economy of corporations', and an international scenario where asymmetric security threats require more and more asymmetric responses.

As a field of research and practice traditionally anchored to a risk management perspective—that is, a focus on avoiding losses—modern information security has the potential to become a value-creating organisational function and, in the long run, a possible source of competitive advantage for companies that do it well. What can companies do to prepare for this? This presentation explores a six-way framework for changing the ways in which individuals, organisations and governments perceive information security, with the purpose of delivering value for consumers, companies and societies.

The knowing-doing gap: Is knowledge enough to prevent cyber-fraud victimisation?

Lucy Farrell, School of Criminology and Criminal Justice, Griffith University, Queensland
Jacqueline Drew, School of Criminology and Criminal Justice, Griffith Criminology Institute, Griffith University, Queensland

This presentation reports on research examining actual victimisation risk, perception of victimisation risk, and knowledge and use of hard (physical) barriers and soft (behavioural) barriers to prevent cyber-fraud. Based on the findings from a survey of 218 participants, despite accurate perceptions of risk and levels of concern, those most at risk of victimisation were found to use fewer hard and soft self-protective measures than those with lower risk of victimisation. Counterintuitively, this study found that having knowledge of self-protective behaviours in the online environment did not translate into the actual use of crime prevention strategies. Based on this research, important conclusions are drawn about the policy implications for those responsible for cyber-fraud prevention. A cybercrime prevention agenda is proposed that focuses on better translating education of potential victims into a meaningful reduction in cyber-victimisation.

The motivations and challenges of reporting online fraud to the "fraud justice network"

Dr Cassandra Cross, School of Justice, Queensland University of Technology

Fraud is unique in that there are a large number of agencies in addition to the police that victims can report to, known as the 'fraud justice network'. It is well established that online fraud has one of the lowest reporting rates across all crime categories. There are several reasons for this, such as the multiplicity of agencies, people not knowing they are victims, and victims believing that nothing can be done, to name a few. While the barriers are well known, it is not known why some victims choose to report online fraud offences and what factors motivate or support victims to come forward.

This presentation examines the under-researched group of online fraud victims who reported their crimes to authorities. Based on interviews with 80 victims across Australia, each of whom lost at least $10,000 to online fraud, this presentation highlights two main motivating factors behind the reporting of online fraud. The first relates to an individual's sense of justice, and the second stems from an altruistic notion of protecting others.

The presentation also highlights the barriers and difficulties encountered by victims when attempting to report the fraudulent incident. Consequently, it details the overwhelming negativity associated with the reporting process. The presentation uses these findings to determine what can be learnt from the victims who were willing to report.
It concludes with a discussion of the challenges evident in seeking to improve the confidence of victims reporting to authorities.

The Playpen cases: computer network operations and extraterritorial criminal law enforcement

Ian Warren and Adam Molnar, Alfred Deakin Institute for Citizenship and Globalisation, School of Humanities and Social Sciences, Deakin University, Victoria
Monique Mann, Crime and Justice Research Centre, School of Justice, Faculty of Law, Queensland University of Technology

Playpen is one of many clandestine networks for the online distribution of child exploitation material. As with the Silk Road illicit drug crypto-market, Playpen relied on The Onion Router network to encrypt and anonymise the internet protocol addresses and geographic locations of site users. The challenges to conventional policing methods presented by these aspects of darknet infrastructure have prompted various enhanced investigatory and intelligence gathering strategies, such as computer network operations (CNOs), to assist with detecting and investigating serious crimes with an online dimension.

These forms of online surveillance, disruption and attack readily transcend multiple legal jurisdictions and test established thresholds governing online policing activities and the admissibility of digital evidence in criminal trials. Criminological literature and judicial rulings are yet to reconcile the contradictions presented by enhanced governmental online surveillance and hacking through existing due process safeguards in both domestic and extraterritorial criminal investigations.

This presentation examines a series of United States cases scrutinising the Federal Bureau of Investigation’s (FBI’s) use of CNOs to identify and prosecute Playpen users located within and outside the US. It describes how the warrants authorising the FBI to seize the Playpen site tacitly authorised the deployment of CNOs to identify site users through the darknet. This generated several conflicting US judicial rulings that attempted to determine an appropriate legal scope for the domestic and extraterritorial use of CNOs.

The presentation looks at the shifting legal boundaries of such operations and their impact on accessing admissible digital evidence when police investigate serious online criminal conduct. Discussion will conclude with a suggestion about how these issues offer insight into current and future developments in online policing, including the due process implications of recent amendments to US criminal procedure that authorise extraterritorial governmental hacking by US security and policing agencies.

Transnational online crime, extradition and human rights: An analysis of US–UK cases for cyber offending

Monique Mann, Queensland University of Technology, Queensland
Ian Warren and Sally Kennedy, Deakin University, Victoria

This presentation describes legal and human rights considerations for suspects involved in serious transnational online offending who have been sought for extradition by the United States from the United Kingdom. An analysis of high-profile cases involving individuals with serious mental disorders and autism shows how recent developments in UK extradition policy pose a series of legal and human rights concerns. Online offending creates new challenges that are not met by established protections underpinning the philosophy of domestic and internationally sanctioned approaches to extradition and human rights. This presentation discusses how the hybrid nature of extradition law and procedure is a highly problematic aspect of contemporary extradition processes in the context of online offending. These issues have implications for future criminological research, online policing and transnational criminal law reform.

Virtual currency and cybercrime

Tala Stevens, Australian Criminal Intelligence Commission

Virtual currency is intrinsically linked to financially motivated cybercrime and is attractive to cybercriminals due to its pseudo-anonymous nature. While virtual currency is pseudo-anonymous, criminals are exposed when they exchange their virtual currency for real money.

This presentation outlines the methods cybercriminals use to exploit virtual currency and covers:

- the global and Australian virtual currency context
- regulation of virtual currency exchanges
- methods used by criminals to exploit virtual currencies to make illicit profits
- virtual currencies other than bitcoin
- future trends in cybercriminal use of virtual currency.

Young adults' perceptions of and engagement with online pornographic material in Australia

Dr Nadine McKillop, University of the Sunshine Coast, Queensland
Dr Julianne Webster, Griffith University, Queensland
Professor Sarah Brown, Coventry University, United Kingdom

The availability, exposure to and consumption of pornography has proliferated since the advent of the internet. Although studies have investigated the extent, nature and trajectories of online pornography use, little research has been conducted on this issue in Australia. To this end, this research investigated young adults' exposure to, perceptions of and engagement with online pornographic material. This presentation will disseminate the findings of research involving 288 participants aged 18 to 25 years.

Participants completed a confidential online survey about their general use of the internet, the content they accessed online and their perceptions of its regulation. A large majority (88 per cent) reported that they had inadvertently been exposed to sexually explicit material while online, mainly in private settings such as homes and on private devices. The average age at first exposure was 13 years old. Almost three-quarters of those surveyed (74 per cent) also admitted to intentionally accessing this material online, with both men and women accessing pornography. The content viewed varied, with nearly one-quarter (23 per cent) reporting watching pornographic material that included sexually violent themes, including rape.

These findings suggest that exposure to and engagement with online pornography is prevalent among young Australian adults. Although many young people know the risks involved in engaging with this material online, they do not appear to be concerned about the nature of the content or their anonymity as a user. This has implications for primary and secondary prevention initiatives regarding safe use of the internet and increasing the perceived risks associated with engaging with this content online.