




# Human Factors, Self-awareness and Intervention Approaches in Cyber Security When Using Mobile Devices and Social Networks

Ken Eustace<sup>1</sup> , Rafiqul Islam<sup>1</sup>, Philip Tsang<sup>2</sup>, and Geoff Fellows<sup>1</sup>

<sup>1</sup> Cyber Security Research Group, Charles Sturt University, Boorooma Street,  
Wagga Wagga, NSW 2678, Australia  
{keustace, mislam, gfellows}@csu.edu.au

<sup>2</sup> Web Consortium Education Foundation, Hong Kong, China

**Abstract.** This paper will describe three case studies on the human factors, in personal and public safety and cyber security from the Asia Pacific region (APAC). A deeper consideration of human factors, the impact of “Internet of Things” and cyber security education about the behaviour and actions that can be taken by individuals is at the foundation of public safety and cyber security. The growth of disruption by cyber criminals - especially when using small devices and applications to interact with large social networks is a cause for concern. This is part of the evolving development of a cyber-physical world. The paper presents three case studies and proposes a *Self-awareness and Intervention Model* for public safety and security by increasing and *maintaining* the awareness, understanding and preparedness of cyber security measures by the individual when using mobile device applications to participate in large social systems and concludes by highlighting the importance of including the human factors and message framing alongside the cyber security measures in place.

**Keywords:** Android Application Security · Context-based behavior  
Human factors · Internet of Things · Intervention · Message framing strategies  
People with special needs · Public safety and security · Self-awareness  
Vulnerability monitoring · Wireless access surveys

## 1 Introduction

There are several cyber security perspectives operating on ICT security projects and issues around APAC. On June 21, 2013, the Australian Government announced that cyber security will be one of the top priorities as part of 15 new Strategic Research Priorities for Australia with a focus on safeguarding personal security using partnerships and with responsibilities within the Asia Pacific region and the wider global context.

Guiding cyber security research activity and underpinning the role that Cyber Security research will play as part of those strategic research priorities, is Australia’s Cyber Security Strategy [1].

## 1.1 Improving Cyber Security in the Asia Pacific Region

Research projects involving cyber security are influenced by the transformations and growth of economies in APAC and should seek to identify ways to improve cyber security for individuals, organizations, businesses and scale up to include government, national infrastructure and even bilateral agreements with Asian countries.

Turban et al. [2] stated that CISCO expects that the average global network speeds will double by 2018 with the 5G networks at the top end of data transfer speeds, being offset by the amount of traffic due to mobile devices and social media interactions. This in turn requires new procedures to lower risks and increase security on mobile devices, cloud services and in social media sites.

Prieto [3] found that regional IP traffic for APAC will grow three-fold at 67.8 exabytes/month by 2020 and that 71% of total IP traffic will originate with non-PC devices including tablets, smartphones, and televisions, compared to 47% in 2015. At the same time by 2020, smartphones will generate 30% of total IP traffic, with PC's total IP traffic contribution to fall to 29%. With global networks supporting 16.3 billion devices in 2015 then going up to 26.3 billion devices by 2020, the growth due to the Internet of Things (IoT) that will create changes and more traffic increases. This will be partly due to the growth in video surveillance, smart meters, health monitoring and wearable applications.

According to Wilkinson [4], most cybercrime legal structures and cyber maturity [28] throughout the APAC region are not adequate to combat issues such as data and identity theft, child exploitation and ransom-based attack and that this is compounded with limited international support between the countries that face the burden of rampant digital criminal activity.

Online deception in social media, as one example, has more to do with human behaviours and education rather than use of intrusion detection and prevention technologies. According to Tsikerdekis and Zeadally [5], online deception in social media involves the cyber threat actor being:

*“Unknown and invisible, ready to exploit the unwary and uninformed and seeking financial gain or reputation damage”*

There is a research interest in safeguarding the personal security and identity management of people using smartphones with particular concern for senior citizens and those with disabilities and in regional Australia, using social media and mobile applications. By building and safeguarding the cyber security awareness and behaviour for all citizens, the resulting improvement would trickle up to improve the other Cyber Security issues in the Asia Pacific region.

There is much concern about cyber security for seniors and people with special needs as the global trend shows that more seniors than ever before will be accessing technology: at home, on the move with smartphones and small devices or in aged care facilities, according to Harvie, Eustace and Burmeister [6–8]. This trend is likely to be encouraged as service providers use electronic interaction in order to save costs and more seniors and people with special needs expect online access to services.

## 2 Case Studies

The human factors associated with public safety and security are complex so we use three case studies to describe issues surrounding vulnerable people, application security and the ease and use of urban wireless access points.

The *Vulnerable People* case is about safeguarding the personal security and identity management of vulnerable people with using social media and mobile applications. The case study examines what strategies and behaviours can be taken to safeguard the independence, privacy, security and identity of people with disabilities, seniors or those in aged care.

The *Android Application Security* case changes the perspective and examines the security issues surrounding the popularity and growth of Android applications on smartphones and deals more specifically with application security on Android devices.

The final case is about *Wireless Access Points* and features the 2015 Wi-Fi Air, Sea and Land Survey in Hong Kong. The focus of this study is on the value of taking action on monitoring, understanding and educating about the adjacent wireless environment and its risks and vulnerabilities.

### 2.1 The Vulnerable People Case Study

The support and training in social media and mobile applications given to seniors and people with disabilities must include awareness and understanding of cyber threat actors and other cyber security issues. Phahlamohlaka's [9] interest on information warfare also included aspects of other research work on human factors and the socio-economic challenges for rural development as regional communities change with the increased use and wireless technology, connectivity and information [19]. What was happening in regional and rural South Africa may have similar effect regional and rural Australia as broadband and wireless cell phone networks expand by 2020 as part of a National Broadband Network (NBN). Those seniors and people with disabilities living in regional and rural areas face double jeopardy and may be part of the *Cyber Security Awareness Divide* as suggested by Connolly et al. [10].

Once we have in place the cybersecurity awareness and behaviours for seniors and people with disabilities then follows a program of wider education and strategies for building awareness and training needs of personal ICT security for all by using the phases for a cyberattack as a template or model for behavioural response and action in each phase. Developing a *Self-awareness and intervention Model* and maintaining the awareness, understanding and preparedness of cyber security measures by the individual begin with prevention measures. Then the *Detection* phase in cyber security can act as the *guardian* for the individual.

By adapting a simplified cyber-security model, after Stallings and Brown [11] based upon the common cyber security phases of Prevention + Detection + Response + Recovery, then each individual can follow a sequence of context-based behaviors to safeguard their data and identity during the four main phases and develop a *Personal Cyber Security Awareness and Intervention Model (PDR<sup>2</sup>)* that is based on a set of context-based

strategies and behaviours to strengthen each link in the cyber security chain as shown in Fig. 1.



**Fig. 1.** PDR<sup>2</sup> is a Personal Cyber Security Model of Self-awareness and Intervention that represents a ‘white box’ full of cyber security strategies and behaviours.

While so many businesses and organizations concentrate on the *Prevention* aspect by setting up firewall and protection zones around a wired and wireless network or a password protection schema based on regular password changes every 30 or 60 days and use of advice on password ‘strength’ (weak, medium, strong). In a recent discussion with colleagues in Hong Kong the benefits of the ‘Great Firewall of China’ was on the agenda.

At the same time, ethics and security go hand in hand to protect the privacy of the individual and assist with identity management, particularly with using social media technology. Indeed, identity management is also a concern for groups of people and the organization as whole. Additional safeguards also exist such as the different privilege levels that are given to people who can access the network.

However, a lot of ongoing protection can tend to be passive after a while as there is a tendency to just *setup and leave* the protection controls in place, even though all the protection measures are warranted, one is left to question how much of the individual, group or organization focus in on the more continuously active *Detection* phase of the model?

In business, government and large organizations like a university, the cyber-security effort is on a much larger scale than the home or office network and is targeted towards the protection of intellectual property (IP) and corporate data stores. In the latter case, so much of the new or cutting edge IP development is done by postgraduates enrolled in a course at the Doctorate or Research Masters levels.

Similarly, if we examine the *Response* phase of the model, then a lot of global support is available via the efforts done by CERT. The Computer Emergency Response Team (CERT) offers to members a coordinated, active, up to date response to vulnerabilities on the network by releasing regular ‘alerts’ to problems as they emerge. Such quick alerts to vulnerabilities due to new malware or security holes in operating system and application software updates are quite effective in maintaining alertness in the behaviour of individuals. Getting the right balance is vital and shaped by the amount of time, resources and budget that an individual can apply or endure, while also affected by the overuse of protection and detection that will see the user experience and benefits reduced

as security levels are increased. The result by going too far may a fortress attitude so there is a need to balance the detection measures so that they act as the effective guardian or the sentinel on the watch acting in the best interests of the individual, the group or the organization.

The use of good detection methods will provide the data to support the decisions made by the individual, the group or the organization and act as a feedback loop to the protection and response phases of the model. The perception with business and organizations may be that the stakeholders only take notice when an incident occurs, acting as bystanders at an accident or fire scene.

Such behaviours may be compared to the behaviour of individual, groups or organizations involved during fire or bomb scare drills. The behaviours will differ from the drill when the threat is real. Such training is a drill and the practiced behaviours may not resemble what happens in the real situation. It is proposed that the detection phase as the ‘guardian’ will provide the data, information and experiences needed for the other prevention and response phases in the personal cyber security model.

De Bruijn and Janssen [12] suggest that our daily dependence on ICT has created the *cyberphysical* society, and that the need and demand is now greater to understand the complex and varied aspects of cyber security. They also propose the use of an evidence-based message framing strategy is needed to *frame cyber security*, similar to the use of the three case studies in this paper. Six communication strategies were identified by De Bruijn & Janssen as providing a way to frame or explain cybersecurity (See Table 1).

**Table 1.** The communication strategies that can be used to explain cybersecurity to the community.

	Six communication strategies by De Bruijn and Janssen [12]
1	<i>Do not exacerbate or worsen cybersecurity</i>
2	<i>Make it clear who the villains are</i>
3	<i>Give cybersecurity a face by putting heroes in the sunlight</i>
4	<i>Connect cybersecurity to values other than security alone</i>
5	<i>Personalise the message for easy recognition</i>
6	<i>Connect to other tangible and clear issues</i>

However, communication strategies 2 and 3 presents some risk. In *making it clear who the villains are*, we risk promotion and copying by others, while in *putting heroes in the sunlight*, we risk making them targets for attack. By educating and communicating the benefits of learning and using a simple personal cyber security model to each individual in a community, each person including seniors and those with disabilities, can exercise the personal cyber security to maintain or change to a set of behaviours in their own personal cyber-security model.

The issues around privacy and identity management exist in the use of social media technology (mobile apps), so all of us need to be aware and to learn how to apply our own personal version or instance of the simple personal cyber security model. Without implementing a personal cyber security model or bothering to learn what behaviours are appropriate then the growth of cyber-security vulnerabilities can continue and Recovery

times and the risks increase. This is where cyber security experts get involved in education and policy making through use of ideas like De Bruijn & Janssen's ideas [12] about the use of better communication by education and message framing strategies that help understanding by removing ambiguities.

Such a model should also be context-based and be developed as a user-centred model where each individual takes ownership of his or her own personal cyber security model. If the user-centred approach together with good message framing techniques can be made to work in tandem for those disadvantaged people in the community then it should be horizontally and vertically scalable to other people, groups, organizations using social media in our cyber physical society.

Some disadvantaged people and those in aged care have wearable devices for medical, rehabilitation or fitness purposes. This calls into question the security and privacy risks wireless protocols for medical devices (pacemaker, defibrillator) even though safeguarded by legislation and manufacturer *third party* protocols. The growth of wearable bands for fitness designed to use social media and cloud storage of personal fitness data so the user can download and view, also includes GPS data for tracking. The risks in information sending by the user coupled with storage and retrieval may mean the data can be read without anyone knowing. Just who owns the personal health data?

The use of trusted parties and privacy policy needs to be included with all wearable devices before the advent of whole body networks (WBN) using linked wearable devices such as a fitness band, a pacemaker and device a retinal implant. If all the individual personal cyber security models were in place and connected then each node in a WBN may re-enforce the next by working as a cyber-security mesh in practice.

## 2.2 The Android Application Security Case Study

Turban et al. [2] described how a botnet of Android phones was used to send large volumes of spam via Yahoo e-mail servers - using SMS as the "command and control channel". The era of the Smartphone has arrived and these devices permeate into every aspect of our daily lives, the importance of establishing effective security measures becomes increasingly important. In this literature, we analyse the current security systems in place, their evident shortcomings and the proven potential malicious or unsolicited behaviour. The streamlined nature of the application marketplace and rigid security implementation combined with a general lack of awareness and comprehension of security implications amongst end users is a legitimate cause for concern. There is a critical need for a revised security strategy surrounding the Android application framework and a number of proposed solutions are examined.

StamMBERger [13] summed up the ubiquitous trend of smart devices in one simple statement:

*"PCs are no longer the dominant form of computing"*

Preito [20] supports the rise of the smart devices with the CISCO data that showed that by 2020 then smartphones IP traffic will exceed that of PCs. As far back as 2008, mobile broadband connections had increased and exceeded that of fixed broadband subscribers and by the end of 2009 there were an estimated total of 4.6 billion cellular subscriptions

worldwide according to the U.S. Department of Homeland Security [14]. Since then the popularity of smart phones has risen exponentially along with the popularity of mobile phone applications.

On Android-based devices, applications are predominantly downloaded and installed via the Android Market although other markets do exist such as Amazon's Appstore. On July 14 2011, it was reported by Nickinson [15] that the Android Market had surpassed 250,000 applications and over 6 billion downloads. Enck et al. [16] suggested that the:

*“low barriers [for developers] to bring applications to market, and even lower barriers for users to obtain and use them”*

has undoubtedly promoted this uptake. Indeed, for a small fee, developers are able to freely produce and distribute applications in what is widely regarded as the “*unmoderated Android market*” according to Vidas et al. [17].

Dissimilar to desktop Operating Systems, applications on Android are treated as “*mutually untrusting, potentially malicious principals*” – as described by Felt et al. [18] requiring specific permission to be granted once only during install-time. End users are shown a page just before installation listing the applications requested permissions at which time they may accept all permissions and proceed or decline cancel the installation completely. Permissions are displayed in three layers; categories, specific permissions and a hidden details dialog. A survey conducted by Felt et al. [19] concluded that the categories were so broad that they caused users to over-estimate the implications resulting in “*a negative impact on the amount of attention that users pay to [specific] permissions*”.

More worrying perhaps was the fact that 42% of the lab study respondents were completely oblivious to the existence of such permissions with one user saying “I don't ever pay attention. I just accept and download it” Felt et al. [19]. This trend is possibly facilitated by the “*streamlined*” nature of the current market. However, end user complacencies are not the only area lacking. Even for a technically minded individual the vague permission descriptions fail to provide sufficient information for effective decision making. One such respondent with a small amount of experience as an Android developer commented (Felt et al. [19]):

*“I've done some programming but I don't know all the permissions. ... I just don't know if the permissions are so fine grained that they make texting a special permission that you have to add”*

Overall, the current mechanisms in place are severely inadequate and simply too rigid. Essentially, when installing an application of undetermined integrity, a user must decide, or more fittingly take a somewhat educated guess, whether or not the permissions being requested are appropriate based on a single page of largely misunderstood permission descriptions and implications. In some cases, user reviews can assist users in making a decision but that requires actions and knowledge on behalf of other users and is by no means a satisfactory solution.

The potential for, and evidence of, unscrupulous application behaviour is all too real and unfortunately, largely underestimated. Stammberger [13] warns of a “*Dangerfield Paradox*” where the continuing abundance of PC-based attacks diverts attention away from devices “*despite the inevitability, importance, and difficulty of solving*” this arising

issue. In fact, the issue has largely arrived already, with the same survey revealing that of the 269 respondents:

*“65% report that attacks against their smart devices already require the regular attention of their IT staff, or will start requiring it this year. In fact, 23% of organizations surveyed already repel device attacks at least once monthly, while 10% must do so on a daily basis”* (Stammerger [13])

It also reveals the growing uncertainty amongst users with 77% expressing some level of concern about current mobile phone security. This concern is well-founded and justified by several other research articles which investigate the various exploitable aspects of the Android application framework as it currently stands. Areas of primary focus are the misuse and collection of sensitive and personal information, application permission re-delegation which undermines user-granted permissions themselves and the penetration of advertising and analytic libraries.

Enck et al. [16] developed a decompiler to extract 21 million lines of code from the top 50 applications across each of the 22 application categories for analysis (as of September 1, 2010). This comprehensive examination *“uncovered pervasive use/misuse of personal/phone identifiers, and deep penetration of advertising and analytics networks”*. Such networks were found to be integrated into over half of the applications studied. An alternate taint tracking method, TaintDroid, was used to report similar findings. TaintDroid,

*“automatically labels (taints) data from privacy-sensitive sources and transitively applies labels as sensitive data propagates through program variables, files, and inter-process messages”* Enck et al. [20]

and records this data as it attempts to leave the system. Although a significantly smaller sample size of just 30 popular applications, *“68 instances of potential misuse of users’ private information across 20 applications”* [20] were detected. The penetration of advertising networks was also apparent with half the applications attempting to report the user’s location to remote advertising servers, occasionally with additional private data such as IMEI or phone numbers.

Both studies reported *“an overwhelming concern for misuse of privacy sensitive information such as phone identifiers and location information”* (Enck et al. [16]). They revealed that phone identifiers are being transmitted and used for a whole range of purposes from *“cookie-esque”* tracking to account numbers and were frequently leaked in plain text and *“finger-printed”* on remote servers (Enck et al. [16]). It was also reported that IMEI numbers are often tied to personally-identifiable information discrediting *“the common belief that the IMEI to phone owner mapping is not visible outside the cellular network”* (Enck et al. [16]).

The probing of permissions was also a suspicious and widespread occurrence. This activity was found to be instigated from not only advertising and analytical libraries, but also from some developer toolkits which can lead to dangerous functionalities appearing in *“well-known”* branded applications. For example, the *“CBS Sports Pro Football”* application was found to exhibit permission probing behaviour whilst *“USA TODAY”* and *“FOX News”* programs were found to access IMEI data due to the developer toolkits used (Enck et al. [16]).



From all this we can derive one common theme that, as pointed out by Enck et al. [20],

*“resolving the tension between the fun and utility of running third-party mobile applications and the privacy risks they pose is a critical challenge for smartphone platforms”.*

Enck et al. [20], goes on to list the major challenges of protecting sensitive data on a Smartphone. Firstly, smartphones have limited resources restricting the *“use of heavy-weight information tracking systems”* (Enck et al. [20]). The interactivity between applications on a device also present difficulties for monitoring systems to be able *“distinguish multiple information types, which requires additional computation and storage”* (Enck et al. [20]). Also, the dynamic nature of context-based information can be hard to identify. Enck et al. [20] points out that *“for example, geographic locations are pairs of floating point numbers that frequently change and are hard to predict”*.

Enck et al. [20] claims TaintDroid to *“provide a novel, efficient, system-wide, multiple-marking, taint tracking design by combining multiple granularities of information tracking”* but is quick to point out

*“like similar information-flow tracking systems, a fundamental limitation of TaintDroid is that it can be circumvented through leaks via implicit flows”.* Enck et al. [20]

This of course being a sign of malicious behaviour itself and potentially detected via other means such as static analysis. An observed, major obstacle, especially for a real-time monitoring system such as TaintDroid is keeping performance overhead to a minimal and acceptable level. TaintDroid claims *“only 14% performance overhead on a CPU-bound micro-benchmark”* (Enck et al. [20]) and although this is painted in a positive light, would still appear to be quite a footprint when considering that this would be consistently monitoring in the background.

Other possibilities were briefly but critically analysed by Felt et al. [18]. Mandatory Access Control (MAC) systems propose a hierarchy of integrity and confidentiality levels where the flow of data between different levels is restricted (Felt et al. [18]). Although, sound in theory, the Android framework is too complex and applications would transcend various levels simultaneously thus resulting in a confusion of the policies and a possible deadlock between the requester and deputy.

Stack Inspection has the advantage of being able monitor *“confused-deputy”* attacks during run-time but also comes with several limitations. These are specified by Felt et al. [18] as the Stack Inspection being *“dependent on the runtime for correctness”* and having to *“be re-implemented repeatedly for a system with multiple types of runtimes”*. History-Based Access Control is similar in operation, relying on runtime mechanisms, and *“reduces the permissions of trusted code after any interaction with untrusted code”* (Felt et al. [18]).

It is obvious that Android and its associated marketplace and applications have reached a level of ubiquitous that has attracted, and will continue to attract, unscrupulous individuals and activities. The explosion and uptake of this technology has left security behind and appropriate measures and standards need to be put in place to prevent the inevitable scamming and malicious attacks. This issue needs to be addressed sooner rather than later. Due to the complex and mutually untrusting relationship between the Android OS and its third-party applications, this solution will need a multi-faceted approach and poses some challenging obstacles. The end result will likely need to be a

collation of a number of proposed solutions, possibly the combination run-time monitoring, static analysis and application certification.

### 2.3 The Wireless Access Points Case Study

This final case study describes the Wi-Fi Air, Sea and land Survey of Hong Kong SAR. It presents the rationale and the main findings of a quantitative study of a longitudinal Wi-Fi security survey in Hong Kong, China (Fig. 2). The authors have been conducting one of the world's most comprehensive longitudinal Wi-Fi surveys in HK since 2002 (Tsang et al. [21]; Tsang and Eustace [22]). This survey has looked at the different ways that one can visualise Wi-Fi Access Point data, to see how it is distributed within a city or an area and to draw conclusions about its use by means of mapping. Air and Sea data was collected by helicopter using Laptops and a Raspberry Pi. This was complemented by land survey data collected by foot (Android smartphone) and by car (war driving).



**Fig. 2.** 2015 Wi-Fi Helicopter Survey Meeting Place: Clipper Room, Peninsula Hotel, Kowloon 1:45 pm 12 April 2015. The helicopter and team of researchers and students involved in the 2015 Wi-Fi Survey in Hong Kong.

The findings will be of interest to security experts and ICT educators in general. In 2015, we are already seeing the move from IEEE 802.11n on both the 2.4 GHz and the optional 5 GHz bands to the enhanced IEEE 802.11ac (5G Wi-Fi), making the 2015 Wi-Fi Air, Sea and Land survey valuable as a baseline study for the growth in use of 5G Wi-Fi. The industry partners in this project included HK Technology Exchange Limited, HK Technology Association, Web Consortium Education Foundation & Heliservices Limited

and the objectives of the 2015 Wi-Fi Air, Sea and Land Survey of Hong Kong are shown in Table 2.

**Table 2.** Wi-Fi air, sea and land survey of Hong Kong objectives

Wi-Fi air, sea and land survey of Hong Kong objectives	
1	<i>Setting a new world record for a Wi-Fi survey</i>
2	<i>Surveying the latest trend in usage and security awareness in Wi-Fi and wireless communications deployment</i>
3	<i>Connecting with business sponsors on the use of secure Wi-Fi access points</i>
4	<i>Provide hands-on authentic work experience conducting a Wi-Fi Survey</i>
5	<i>Formulating practical educational values from a Wi-Fi experiment</i>
6	<i>Providing leadership in wireless LAN survey methodology</i>

A variety of network technologies such as Bluetooth, Wi-Fi, WiMAX, ZigBee, NFC and RFID technologies exist in Hong Kong, providing some unique cyber security risks and issues concerning the communications medium. Data transfer occurs via radio waves and so the wireless environment has several points of attack including the wireless device, the access point (AP) and the transmission medium for the radio waves.

Fong and Wong [23] conducted a questionnaire survey of 207 participants on Hong Kong Wi-Fi Adoption and Security in 2014 and suggested that while Wi-Fi is easy and convenient for, knowledge gaps exist in using and setting up a Wi-Fi service. Vulnerabilities will exist if the network is not secured. With the on-going development of the “Internet of Things”, Wi-Fi cyber security measures and education programs should be expanded along with the more secure use of location-based NFC mobile payment services.

Raspberry Pi and Android Phone performance was better on the land survey than the use of two configurations of laptops with high gain antenna in the air and sea survey by helicopter. Table 3 the results that display some concern for the human factors about security and privacy issues. Such vulnerability monitoring surveys must be held on a regular basis.

**Table 3.** The main results from the 2015 Wi-Fi air, sea and land data collection environment in Hong Kong

Air and sea survey	Land survey
<p><i>3 data sets (air) and 4 data sets (sea) of SSIDs were combined with duplicated MAC addresses filtered out</i></p> <p><i>7133 Access Points (AP) detected</i></p> <p><i>90% of APs used 802.11n</i></p> <p><i>70% of APs used WPA/WPA2 security and 30% were open (a privacy concern in restaurants and hotels without guest authentication)</i></p> <p><i>3G/4G APs from mobile devices (Wi-Fi modem or mobile phone hotspots were discovered (MACs and SSIDs)</i></p>	<p>Data sets were combined from Raspberry P1 2 and Android smart phone with WiGLE to collect the SSIDs</p> <p>31 350 APs collected</p> <p>97% used 802.11n</p> <p>75% of APs used WPA/WPA2 security and 25% were open and several open SSIDs were from wireless printers (another privacy concern)</p> <p>2% of SSIDs came from mobile phone Wi-Fi hotspots. Xiaomi, Samsung and Apple were most common brands</p>

If we use 2014 as a reference year prior to the Wi-Fi survey, Symantec [24] observed that the cyber security threats in 2014 of concern included that 17% of all Android apps (nearly one million total) in 2014 were actually malware in disguise and that 70% of social media scams were manually shared. The number of data breaches increased 23% in 2014 E-crime and malware via ransom-ware attacks grew 113% in 2014. Table 4 below shows the relative black market value of stolen access or information in 2014 as trading continues on the dark Web and elsewhere.

**Table 4.** Value of information sold on black market (Symantec [24])

Item	2014 value \$US
<i>1,000 Stolen Email Addresses</i>	\$0.50 to \$10
<i>Credit Card Details</i>	\$0.50 to \$20
<i>Scans of Real Passports</i>	\$1 to \$2
<i>Stolen Gaming Accounts</i>	\$10 to \$15
<i>Custom Malware</i>	\$12 to \$3500
<i>1,000 Social Network Followers</i>	\$2 to \$12
<i>Stolen Cloud Accounts)</i>	\$7 to \$8
<i>1 Million Verified Email Spam Mail-outs</i>	\$70 to \$150
<i>Registered and Activated Russian Mobile SIM Card</i>	\$100

Knowing how cybercriminals are threatening security is the first step to securing information. From social media vulnerabilities to acts of digital extortion, it can be suggested there are threats that now extend the existing wireless network threats. Up to five types of attackers have been identified in network security:

1. the *script kiddy* (an unskilled individual who uses scripts developed by others),
2. the *knowledgeable enthusiast*,
3. the *criminal hacker*,
4. the *idealist* with a cause,
5. black-budget *funded sovereign-state employee*.

The latter attacked is the most dangerous and is usually drawn from the ranks of the previous four types. This attacker has the best motivation, the time, and the funds to breach any system via the internet and others systems with brief physical access using USB ports or other ports such as thunderbolt with purpose-built devices. Any system that attaches to the internet or is taken outside is vulnerable. Even charging a laptop at an airport charging station gives an access point for an attack.

### 3 Conclusion and Discussion

The human factors associated with public safety and security were explored using three case studies from the Asia Pacific region to describe issues surrounding vulnerable people, application security and the ease and use of urban wireless access points.

The *Vulnerable People, Android Application Security and Wireless Access Points* case studies bring forth the human factors at work and some essential cyber security

strategies and behaviours as well as a need to know and understand the adjacent wireless environment by all Internet users and organisations. The development of a Personal Cyber Security Model of Self-awareness and Intervention that represents a ‘white box’ full of cyber security strategies and behaviours, requires localised community education and training programs that will build trust and respect for others, especially in using wearable devices, health monitors and in all social media and online gaming communities. Such heightened and maintained awareness will help users to have discretion when sharing data and stop data leakage from poor user behaviour.

However these essential human efforts must also couple tightly with the evolving cyber security strategies and policies. The Android application security wireless access points studies showed the need for sandboxing, run-time monitoring, static analysis and application certification and at the same time a needed to know and secure local Wi-Fi access points. The use of encryption and firewalls, password and query statement strength as well as biometrics and other procedures for verification and authentication is only the start. The volume and change of threat tactics as network traffic increase via the Internet of Things, will also lead to an increased diversity of devices and applications, sensors and devices using the ZigBee protocol networks, requiring security measures beyond the Wi-Fi protocol networks as well as malware, denial of service attacks, phishing awareness and detection.

Cybercriminals are targeting social networks, smart devices and mobile applications via wireless networks. Smartphones, tablets and even television sets - all need stronger defences or authentication processes for the control of remote access and connections to cloud services. Turban et al. [2] suggested that some minimum security defences for mobile devices already exist (Table 5).

**Table 5.** Cyber security minimum defences for mobile phones and devices.

<b>Minimum Defences</b>	
<b>Authentication</b>	Voice and fingerprint biometric integrated with the operating system/device interface.
<b>Malware Detection.</b>	Constant rogue App monitoring at the main App stores to detect and destroy malicious apps.
<b>Loss or theft of Device.</b>	Mobile <i>kill switch</i> or remote erase capability option is available from smartphone platform

The way that social network sites grow into large social systems has increased, so too has the need for more personal action in regard to personal cyber security. Starting with improved and context-based individual and group behaviours, the personal cyber security model is one way that the individuals may safeguard and standardise their own cyber security safety and goes beyond being a strategy model to scaffolding user behaviour. As information warfare and e-crime around the world is increasing along with large scale surveillance measures to stop the leakage of intellectual property and classified information, each individual must also install, upgrade or refine their own cyber security at the personal level.

The authors propose that the role of Detection in cyber security can act as the guardian for the individual, by adapting a simplified cyber-security personal cyber security model [11] then each individual can follow a sequence of context-based behaviours to safeguard their data and identity. Safety in numbers is a true idiom when an individual connects online then each node in the social network is also affected and the

security levels ‘cascade’ as the community grows and helps to lower the paranoia and concern of also being part of a larger social system. Fellows et al. [25] discussed how ICT security techniques and human factors can work together to lower any concern that the individual may have in being an active member of a large social system. They suggested that the personal cyber security model will work best if the importance of human factors is considered alongside with the technical ICT security strategies.

The use of encryption of data and SSID passwords are among the technical measures, that must be accompanied by the use of discretion by the individual when sharing information and stopping any leakage, as other members of the social network may share with other networks who would not be part of the original intention to share. Recent problems that famous people have had with photos being circulated on Facebook and Twitter are examples of this kind of low level leakage, while Snowden’s leakage of leaking classified documents about U.S. surveillance programs (Shoichet [26]) has shown the consequences when the lack of trust, respect and affection as human factors, is scaled upwards and spread rapidly out of control over social networks.

In conclusion, they suggested that the human factors surrounding the core issues of the leakage problem go beyond all cyber security strategies in place and just boil down to how well each individual is treated by others, by both ‘near’ and ‘far’ neighbours in their multiple social systems. Tsikerdekis and Zeadally [5] suggested that deception prevention begin with harder and standardized user registration and credential verification. Such steps are needed when using social media and safeguarding personal data with wearable devices in a whole-body networking future. By including the human factors and user behaviour in developing cyber security policy and practices with the latest technology for authentication such mobile biometrics, remote erase capability and encryption, can we hope to prevent compromise and deception.

Just as weak security on smart devices are a serious threat, either from intentional or unintentional attacks, so too are people without a high level of self-awareness and intervention control over the security of their near and far network connections. Understanding the human factors and development of human capital play an important role here, requiring mandatory measures for all. Warren [27] stated that human capital is related to situational awareness and incident reaction (personal cyber security model) but also requires development of culture over time as well as the retention and recruitment process of human resources.

In addition, a set of core security technology skills are required. According to Warren [27], the Australian Signals Directorate (ASD) stated that 85% of all targeted attacks could be prevented by four simple mitigation strategies:

1. Application Whitelisting (selected applications, DLLs only)
2. Patching Application updates
3. Patching Operating System updates
4. Restricting Admin privileges based on user duties.

As the network of nodes (device and social networks) for each individual grows into a complex system, giant components will form as the hub or router with access to attributes or properties of other connected nodes (edges). Each node then contributes to develop their own cyber maturity from the bottom up all the way to build and measure the national

cyber maturity, as described by Feakin et al. [28] for cyber security policy the Asia-Pacific Region.

Each device node or human actor must have its security attributes at the top level. So then network security of such a complex system may be simplified as a whole and have better external protection if each of its nodes and actors have high levels of internal security, self-awareness and intervention mechanisms - whether a smart sensor or a human. We need to focus on personal cyber security/identity awareness and behaviours for each citizen. These personal cyber security/identity awareness and behaviours then operate at the individual level each time that a smart citizen interacts via more access points to a myriad of IoT small devices such as Raspberry Pi and Arduino sensor projects come online.

*A Personal Cyber Security Model of Self-awareness and Intervention* can improve defences from the constant security threats by building a mesh of individual secure nodes (human actors), each armed with improved security behaviours and strategies that cluster and build secure networks (defensive nodes) against all cybercrime. Such actionable wisdom is a creative process, providing an operational frame of reference to the cyber security agenda.

Cyber security researchers everywhere also need a special 'dark ethics' policy to defend against making an error of logic, in giving any rights that are forfeited by the behaviour of the cracker or cybercriminal.

## References

1. Australia's Cyber Security Strategy. <https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf>
2. Turban, E., Volonino, L., Wood, G.R.: Information Technology for Management: Digital Strategies for Insight, Action and Sustainable Performance. Wiley, Hoboken (2015)
3. Prieto, R.: Cisco VNI Predicts Near-Tripling of IP Traffic. <https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1771211>
4. Wilkinson, M.: Cyber Security Challenges facing Australia in the Asian-Pacific Region. <http://thinkspace.csu.edu.au/itc571securitychallengesinapac/>
5. Tsikerdekis, M., Zeadally, S.: Online deception in social media. *Commun. ACM* **57**(9), 72–80 (2014)
6. Eustace, K., Burmeister, O.: Ethics and governance of ICT-based social engagement in institutional aged care. In: Seventh Australian Institute of Computer Ethics Conference (AiCE) (2013)
7. Harvie, G., Burmeister, O., Eustace, K.: Bringing the oldest-old into the digital age: overcoming challenges of mobility, literacy and learning. In: 13th National Conference of Emerging Researchers in Ageing. <http://www.era.edu.au/ERA+2014>
8. Harvie, G., Eustace, K., Burmeister, O.K.: Assistive technology devices for the oldest-old: maintaining independence for the fourth age. In: Kreps, D., Fletcher, G., Griffiths, M. (eds.) HCC 2016. IAICT, vol. 474, pp. 25–33. Springer, Cham (2016). [https://doi.org/10.1007/978-3-319-44805-3\\_3](https://doi.org/10.1007/978-3-319-44805-3_3)
9. Phahlamohlaka, J.: Defence, peace, safety, security and information warfare research, In: SCM Seminar Series. Charles Sturt University, Wagga Wagga, NSW, Australia (2012)

10. Connolly, C., Maurushat, A., Vaile, D., van Dijk, P.: An overview of international cyber-security awareness raising and educational initiatives. In: International Cyber-Security Awareness, Sydney (2011). Site: [acma.gov.au](http://acma.gov.au)
11. Stallings, W., Brown, L.: Computer Security: Principles and Practice. Pearson, Upper Saddle River (2012)
12. De Bruijn, H., Janssen, M.: Building cybersecurity awareness: the need for evidence-based framing strategies. *Gov. Inf. Q.* **34**(1), 1–7 (2017)
13. Stammberger, K.: Mobile & Smart Device Security Survey 2010: Concern Grows as Vulnerable Devices Proliferate, Smartphones are the Tip of the Iceberg. Mocana Corporation (2010)
14. U.S. Department of Homeland Security: Technical Information Paper-TIP-10-105-01 Cyber Threats to Mobile Devices, Washington (2010)
15. Nickinson, P.: Android market now has more than a quarter-million applications (2011). <http://www.androidcentral.com/android-market-now-has-more-quarter-million-applications>
16. Enck, W., Octeau, D., McDaniel, P., Chaudhuri, S.: A study of Android application security. In: 20th USENIX Security Symposium (2011)
17. Vidas, T., Votipka, D., Christin, N.: All your droids are belong to us: a survey of current android attacks. In: Proceedings of the 5th USENIX Conference on Offensive Technologies. USENIX Association, Berkeley (2011)
18. Felt, A.P., Wang, H.J., Moschuk, A., Hanna, S., Chin, E.: Permission re-delegation: attacks and defenses. In: 20th USENIX Security Symposium (2011)
19. Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D.: Android permissions: user attention, comprehension, and behaviour, Electrical Engineering and Computer Sciences, University of California at Berkeley (2012)
20. Enck, W., Gilbert, P., Chun, B., Cox, L., Jung, J., McDaniel, P.: TaintDroid: an information-flow tracking system for realtime privacy. In: 9th USENIX Symposium on Operating Systems Design and Implementation (2010)
21. Tsang, P., Kwok, P., Kwong, R., White, B., Fox, R.: Innovation in ICT teaching: a longitudinal case study of Wi-Fi in Hong Kong. *Int. J. Innov. Learn.* **10**(1), 85–101 (2011)
22. Tsang, P., Eustace, K.: Educational and social implications from a longitudinal Wi-Fi security study (2002–2014). In: Proceedings of the International Conference on Information Technologies, InfoTech 2014, Bulgaria (2014)
23. Fong, K., Wong, S.: Hong Kong Wi-Fi adoption and security survey 2014. *Comput. Inf. Sci.* **8**(1) (2015)
24. Symantec: 2015 Internet Security Threat Report. [https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932\\_GA-internet-security-threat-report-volume-20-2015-social\\_v2.pdf](https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf)
25. Fellows, G., McAfee, M., Eustace, K.: The role of human factors in the ICT security of large social systems, Las Vegas USA (2013, Unpublished paper)
26. Shoichet, C.E.: Is Snowden worth the risk? Latin America weighs pros and cons. <http://www.cnn.com/2013/07/11/world/americas/latin-america-snowden-asylum>
27. Warren, M.: Keynote Address, ICT Higher Degree Research Symposium 2016. Charles Sturt University. <https://www.asd.gov.au/infosec/mitigationstrategies.htm>
28. Feakin, T., Woodall, J., Nevill, L.: Cyber maturity in the Asia-Pacific Region 2015. ASPI. <https://www.aspi.org.au/publications/cyber-maturity-in-the-asia-pacific-region-2015/Cyber-Maturity-2015.pdf>