2010

Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats

Nurul Nuha Abdul Molok
University of Melbourne

Shanton Chang
University of Melbourne

Atif Ahmad
University of Melbourne

DOI: 10.4225/75/57b673cf34781
Originally published in the Proceedings of the 8th Australian Information Security Mangement Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

Information Leakage through Online Social Networking: Opening the Doorway for Advanced Persistence Threats

Nurul Nuha Abdul Molok, Shanton Chang and Atif Ahmad
Department of Information Systems
University of Melbourne
Victoria, Australia
n.abdulmolok@pgrad.unimelb.edu.au
shanton.chang@unimelb.edu.au
atif@unimelb.edu.au

Abstract

The explosion of online social networking (OSN) in recent years has caused damages to organisations due to leakage of information by their employees. Employees' social networking behaviour, whether accidental or intentional, provides an opportunity for advanced persistent threats (APT) attackers to realise their social engineering techniques and undetectable zero-day exploits. APT attackers use a spear-phishing method that targeted on key employees of victim organisations through social media in order to conduct reconnaissance and theft of confidential proprietary information. This conceptual paper posits OSN as the most challenging channel of information leakage and provides an explanation about the underlying factors of employees leaking information via this channel through a theoretical lens from information systems. It also describes how OSN becomes an attack vector of APT owing to employees' social networking behaviour, and finally, recommends security education, training and awareness (SETA) for organisations to combat these threats.

Keywords
Information leakage, unauthorised information disclosure, online social networking, social media, advanced persistent threats, cyber espionage

INTRODUCTION

There have been some high profile cases of employees leaking confidential and sensitive information through online social networking (OSN) reported in the media. For example, an Israeli military exposed the location and time of an upcoming raid in his Facebook status update causing Israeli military to cancel the entire operation (BBC, 2010). The same thing happened not once or twice but 16 times in the U.K. done by Ministry of Defence employees exposing British Military secrets to the public via Facebook and Twitter (Mansfield, 2010). In the U.S, a congressman who is also the U.S. House Intelligence Committee member, exposed his secret trip to Iraq when he 'tweeted' his arrival in Baghdad using his mobile and continued posting his whereabouts and the party's itinerary every few hours (Ng, 2009). The leaked information will certainly benefit the adversaries, but at the same time will detriment the organisations.

Irresponsible use of social media causes detrimental impacts on organisations in terms of putting organisations' networks and systems at risk of malware, leading to potential lawsuits due to copyright and defamation, loss of productivity, and significantly impacting on organisations' reputation and future revenue (Colwill, 2010; Gudaitis, 2010; Young, 2010). Recently, OSN has become the target of cybercriminals not only to steal information, but also to use their storage and bandwidth for botnet command-and-control capabilities (Everett, 2010; Smith & Toppel, 2009; Westervelt, 2009). To make it worse, Facebook profiles are now available to be downloaded from torrent sites exposing more than 170 million users' information globally (Paul, 2010).

Furthermore, cybercriminals nowadays are more interested in gathering information, the value of the organisation, than to notoriously taking down networks (McAfee, 2010). Some of them are sponsored by certain parties to do extremely complex attacks to steal sensitive information from the targeted organisations through their employees. They use information available in the public domain, especially online social media to gather as many information on the key individuals before launching spear-phishing and social engineering techniques to obtain credentials for accessing the valuable information (Smith & Toppel, 2009; Sophos, 2010; Symantec, 2010). This threat is called advanced persistent threat (APT) or cyber espionage, although it is not new, it is rapidly growing due to the proliferation of OSN.

Therefore, organisations both large and small, government agencies or private enterprises, need to pay close attention to the use of OSN among their employees. They cannot rely solely on technical controls to combat this problem since it involves human vulnerabilities that need to be safeguarded by behaviour-changing controls such as the implementation of well-enforced information security policies and, security education, training and awareness (SETA).

This conceptual paper explores the phenomenon of information leakage among employees through the use of social networking sites that recently becoming the target of cybercriminals to launch APT attacks. It attempts to answer these questions, pointing at the direction for further research:

1. Why employees disclose organisational information on their OSN sites?
2. How APT attacks on targeted organisations are realised through the use of OSN sites?
3. How do organisations safeguard their information from being leaked by employees through OSN?

With the answers to these questions, we hope to shed some light on individuals and organisations about OSN as one of the vectors to APT attacks and suggest SETA as an approach to address this issue.

INFORMATION LEAKAGE THROUGH OSN

This section provides a brief explanation on information leakage and exerts OSN as the most challenging channel of information leakage. It also attempts to answer the first question: *Why employees disclose organisational information on their OSN sites?* We explain employees' social networking activities which inadvertently and intentionally cause leakage of information and the reasons why this happens based on a theoretical model from Information Systems (IS). This is important to understand the causes of information leakage through this channel since based on this understanding, we suggest a guideline for organisations to mitigate this problem, which will be discussed in the Prevention of Information Leakage through OSN section.

We define information leakage as "a breach of the confidentiality of information, typically originating from staff inside an organisation and usually resulting in internal information being disclosed into the public domain" (ISF 2007, p.2). Although information leakage or unauthorised information disclosure can be caused by malicious and non-malicious insiders, non-malicious insiders are the greater problem (CSI, 2009) since accidental security incidents happen more often and have greater potential for harm than malicious insider attacks (Colwill, 2010).

Academic literature indicates that information can be leaked through OSN (Colwill, 2010; Gross & Acquisti, 2005; Gudaitis, 2010; Leitch & Warren, 2009), face-to-face conversation and printing facilities (Ahmad, Ruighaver, & Teo, 2005), email (Carvalho, Balasubramanyan, & Cohen, 2009), cloud computing (Ristenpart, Tromer, Shacham, & Savage, 2009), domain name systems (Rose, Chandramouli, & Nakassis, 2009) and portable data devices (Colwill, 2010). Among these channels, we view OSN as the most challenging channel of information leakage. This is because information disclosed through OSN creates an opportunity for cybercriminals to do surveillance and gather intelligence, sabotage organisations' networks using malware and utilize resources to launch attacks through the applications on these sites (Colwill, 2010; Gudaitis, 2010; Leitch & Warren, 2009).

While information can be leaked through offline social networking such as meetings, conferences and publications (Jansen, 2010), the leakage through OSN is fundamentally different than its offline counterpart. This is because the moment employees post sensitive information on their sites, the published information is almost permanent, it can be reached by many people and, possibly be copied and distributed to someone else. If they leak information face-to-face to someone, possibly due to the slip of a tongue, the information is confined to the people who heard the conversation, and even if it is communicated to other people, it becomes hearsay.

Typical OSN sites have the functionalities such as status updates, friends' requests, photos and videos uploads, third party applications and links to other websites making them potential avenues of information leakage. Table 1 below shows OSN's capabilities as attack vectors through its available functionalities.

OSN Functionalities	Potential Security Problems	Impacts to Organisations
Post information / update status	Accessibility of OSN by anyone, anywhere at anytime, using any devices, allows users to update their status several times a day, thus, sensitive information may be revealed.	Revealed information can be deduced by attackers to obtain confidential information about the organisations in order to do cyber espionage and sabotage.
Friends' Requests	Carelessness in accepting friends' requests could result to adding 'enemies' instead of 'friends' who have more access to users' information.	These 'friends' are able to constantly monitor the employees' activities within the organisations allowing them to obtain employees' credentials for accessing the corporate network.
Upload photos and videos	Unrestricted photo albums and videos allow everyone to view the photos and videos that are potentially sensitive to organisations.	Sensitive photos and videos may cause embarrassment to the organisations and they may be useful for cybercriminals to collect information.
Third party applications and links to external sites	While using the applications or clicking on the links, malware may infect employees' computing platforms.	Compromised client platforms allow attackers to sabotage corporate networks and provide access to monitor and steal intellectual property.

Table 1: OSN functions and potential problems to organisations

In addition to the above, another characteristic of social media that is similar to other Web 2.0 applications is information in the users' profiles can be leaked by someone else. Users' friends or their friends' friends can post information about them, or copy the posted information, alter the information and possibly distribute it to someone. Similarly, OSN providers can share users' information to advertisers which is common to web advertising practice; the advertisers receive information that is viewed before the user clicked on their advertisement (Jacobsson, 2010). Hence on these sites, "the information on the last page viewed often reveals user names or profile ID numbers that could potentially be used to look up the individuals" (Jacobsson, 2010, p.1). Plus, since many users engage on social networking as their daily internet activities, these sites becomes the primary attention to attackers to launch targeted attacks on organisations and individuals by using spams, phishing and malware through OSN applications (Sophos, 2010). The ability of others to have some control on users' information and the above functionalities make OSN the most challenging channel of information leakage due to the difficulty of managing organisational information that is disclosed through employees' sites.

Although academic literature seldom discusses the information security impacts of OSN on organisations, social networking sites, especially Facebook and Twitter, have made the headlines since 2009 (Goodchild, 2010). Not only that, the concern on this channel as an avenue for security threats is supported by renowned security surveys. For example, the Computer Security Institute (CSI) added 'exploit of user's social network profile' as the new attack type to its 2009 survey (CSI, 2009). Verizon in cooperation with the United States Secret Service (USSS) mentioned in their report that OSN is one of the attack vectors of security breaches (Verizon & USSS, 2010). Plus, Symantec Global Internet Security Threat Report 2009 stated that APT attack begins with reconnaissance through these sites to research on the organisation and its employees (Symantec, 2010). Strengthening this notion, Sophos Security Threat Report 2010 reported that OSN has "become one of the most significant vectors for data loss and identity theft" (Sophos, 2010, p.1).

> "The danger of putting too much personal information online, particularly on social networking sites, was brought to light when the wife of the chief of the British secret service MI6 posted highly revealing details about their residence and friends on her Facebook page" (Sophos, 2010, p.6)

Prior to the above incident which happened in July 2009, organisations were concerned about their employees engaging in OSN because it wasted organisation time and drained the bandwidth, but now, although productivity is still the concern, organisations are more worried about their confidential information being leaked through employees' social networking activities (Gaudin, 2009; Sophos, 2010). As the examples given in the introductory section, even the security-trained people are capable of exposing confidential information that could jeopardise organisational information security. Why do these so-called 'security blunders' happen? In the next section, we explain this phenomenon by using a theoretical model from IS.

THE FACTORS OF LEAKAGE THROUGH OSN

Based on Taylor-Todd's Decomposed Theory of Planned Behaviour (DTPB), an extension to Theory of Planned Behaviour (Ajzen, 1991), IS use is determined by the intention to perform the behaviour. The behaviour intention is driven by these three factors: attitude, subjective norms or social influence and perceived behavioural control.

Attitude towards OSN use

The attitude construct of the model portrays that positive attitude towards IS (in this case, OSN as the social IS) use is based on perceived advantages (usefulness), simplicity (ease of use) and compatibility of the use to their values, experience and needs (Taylor & Todd, 1995). Similarly, individuals and organisations use OSN because it is perceived as a useful tool to them. As it is useful for individuals to maintain close relationship and share information with their friends, it is also useful for organisations to introduce new products and increase reach to customers. Simplicity in using OSN is key to its popularity (Everett, 2010) since anyone, regardless of age and gender, are using OSN adding to 500 million users of Facebook in July 2010 (Facebook, 2010). OSN becomes the platform for employees to solve work-related problems by seeking advice from their friends, which is an example to describe users engage in OSN because it is compatible to their needs. Despite its usefulness, it has a major downside to security. It is also easy for cybercriminals to launch targeted attacks on victim organisations. They can effortlessly find key employees of the organisation, use social engineering methods to befriend them, collect information about their organisations and employees' credentials, and invite the employees to use an application that actually installs Trojans or backdoors to gain greater access into the organisation's networks.

Social Influence

The second construct is social influence from peers and superiors which play a great role on users' participation in OSN. OSN is considered as the in-thing today that not participating in it may be considered outdated. Being influenced by peers engaging in OSN not only blurs the work ethics but also contributes to financial losses. Furthermore, if there is no guideline on the use of OSN in organisations (superior's influence), employees may not realise that they are contributing to the loss of productivity, strains on corporate bandwidth, damage to organisations' reputation, and more serious damages; cybercriminal's sabotage and espionage on the organisations.

Perceived Behavioural Control

While other theories from criminology, psychology and sociology disciplines mostly explain about behaviour that is intentional, DTPB exerts that behaviour can be accidental and intentional since it is performed within and beyond the person's control.

Similar to other insider threats, information leakage through OSN is perceived to be more accidental than intentional especially due to the pervasive use of mobile devices to access social networking sites. Based on the third construct, perceived behavioural control, the intention to perform the IS use behaviour is determined by self-efficacy (perceived ability) and facilitating conditions in terms of resources and technology. As an example to explain accidental information leakage through employees' social networking, consider this scenario; due to productivity concerns, an organisation bans the use of social media during working hours by implementing preventive security systems on their internal networks. Although this mechanism may work to address employees' productivity, they are still able to access their sites using other devices such as ubiquitous smartphones. The 'always on' environment allows employees to constantly update their status, upload photos and videos, and play games, thus inadvertently releasing private work-related information to the public domain.

On the other hand, employees may leak organisational information through social media intentionally with and without malicious intent. For example of an act of malicious intent, a disgruntled employee may disclose proprietary information about their employers or disclose libellous information about the organisation on an OSN site. This is shown by a report by Verizon that a terminated system administrator stole a co-worker's password for his site and modified it with slanderous content (Verizon & USSS, 2010). As an example to intentional information leakage without malicious intent, an employee may deliberately expose the news about the merging of prominent companies before it is formally made public by his employer out of enthusiasm and excitement, or simply to show off.

In this section, we have seen why employees use social media based on the determinants of IS use behaviour from DTPB model. Based on this model, information leakage through OSN is driven by: a) the users' attitude due to its simplicity and perceived usefulness, b) social influence from peers and superior, and c) perceived behavioural control which

explains that while using the IS, the behaviour can be accidental and intentional, due to self-efficacy, available resources and technologies that facilitate the behaviour. The understanding of these underlying factors assists us to propose an approach to deal with this problem. But before that, let's look at how information leakage through OSN provides opportunity for APT attackers to realise their attacks on targeted organisations, making it the most challenging channel of information leakage.

ADVANCED PERSISTENT THREATS (APT)

Aurora attacks, cyber industrial espionage and net reconnaissance are among the interchangeable terms used to describe APT. Although APT is the new term, industrial espionage has existed many years ago and the motives behind it has not changed since, but the technologies to launch the attack certainly have changed (Grabosky, Smith, & Dempsey, 2001). With the rise of OSN users worldwide, it has become the target of APT attackers to initiate their attacks (Gudaitis, 2010; Smith & Toppel, 2009; Sophos, 2010; Symantec, 2010).

APT definitions can vary widely, however, we describe it as a well-funded and well-organised espionage that are financially motivated, employs social engineering techniques and stealthier zero-day exploits to breach networks that are rarely detected by preventive security systems with aims to establish long-term occupying force inside an organisation's perimeter. Typically, APT attackers target financial, government and defence sectors, however, recently large organisations are becoming the target. In January 2010, the media reported that Google, Adobe and other large U.S. organisations were compromised by sophisticated Chinese targeted cyber attacks that appear to be APT attacks. In the attack, intellectual property, email accounts, and other information were obtained and siphoned to other IP addresses in Taiwan (Zetter, 2010).

APT Attack Methods

Usually, this type of attack commences with reconnaissance and information gathering on targeted organisations through identified employees (Smith & Toppel, 2009; Symantec, 2010). The attackers target employees who have access to valuable information and those who are vulnerable; disgruntled employees, employees with financial problem or with weaknesses such as gambling, pornography and drug dependence, who can be induced or coerced to cooperate. With the use of social media, it is not difficult to find out about these characteristics since users are putting up too much information about themselves; personal as well as work-related information (Goodchild, 2010; Sophos, 2010). Furthermore, when collecting information from targeted employees' OSN sites, the information disclosed does not need to be explicit private organisational information, since APT attackers are able to make deductions from non-private information and aggregate them to become very useful and valuable information. They will then use the deduced information to launch attacks on targeted organisations.

Private information on targeted employees can also be gathered through their users' profiles especially when privacy settings are not restricted. Research shows that many users do not impose privacy settings on their profiles, allowing everybody to view their full profiles (Christofides, Muise, & Desmarais, 2009; Gross & Acquisti, 2005; Stutzman, 2006). A study by Ponemon Institute revealed alarming results in which 60% of the surveyed individuals do not screen friends' requests before accepting them, 40% take no steps to protect their privacy and security on social media, and 40% share their passwords with others (Spinney, 2010). These vulnerabilities of OSN users cause APT attackers to easily gather sensitive information about the employees as well as the organisations to realise their attacks.

Once APT attackers have identified the employees, they will use social engineering techniques to obtain valid user credentials (Smith & Toppel, 2009). They will use spear-phishing emails that appear legitimate to trick employees into divulging sensitive information or click on a link or attachment that contains malicious codes. Social media simplifies this by providing the avenues for APT attackers to install and transport malware to the users computing platforms upon clicking on links sent by their seemingly legitimate 'friends' or using applications on these sites. When the malware is installed, it allows the attackers to gain control of the system and access to the network with valid employee credentials that make them undetected (Smith & Toppel, 2009). Hence, employees need to be aware of OSN threats as Gudaitis (2010, p.6) points out, "even a seemingly innocent tweet can lead an unsuspecting user right into a landing page with destructive malware".

In this section, we provide the answer to how APT attacks on targeted organisations are realised through the information being leaked by employees on their social networking sites. Although we are aware that OSN poses other threats to organisational information security, employees' social networking behaviour that can be compromised by APT attackers make this channel a significant vector of this financially motivated attack that can cause serious damage to organisations.

PREVENTION OF INFORMATION LEAKAGE THROUGH OSN

Since information leakage through employees' social networking activities provides the avenue for APT attacks, it is essential for organisations to address employees' behaviour that leads to this problem. This section provides the safeguarding measures for organisations to address this problem and answers the following question: *How do organisations safeguard their information from being leaked by employees through OSN?*

IS security literature proposed information security policy (ISP), security education, training and awareness (SETA) and preventive security systems as key deterrents to insider threats (Bulgurcu, Cavusoglu, & Benbasat, 2010; Straub, 1990; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005; Workman & Gathegi, 2007). Table 2 below shows how these control mechanisms can help organisations to deter employees from leaking information through OSN based on their advantages and disadvantages.

Control Mechanisms	Advantages	Disadvantages
Information Security Policy (ISP)	Well-documented ISP is able to: • clearly define the classification of organisational information for employees to understand the types of confidential and non-confidential information, and how to handle them • specify the rules of the acceptable use of OSN and corporate assets to ensure confidentiality, integrity and availability of information • provide understandable security policies that are integrated with business processes and aligned with job requirements (CISCO, 2008)	• The policy needs to be properly designed, documented, implemented, enforced and reviewed to ensure its effectiveness (ISO/IEC, 2005) thus, requires more resources to mature • Employees' compliance to ISP is determined by the understanding, attitude and beliefs about the severity of security breaches (Bulgurcu et al., 2010; Herath & Rao, 2009; Workman & Gathegi, 2007) • It requires an awareness program to ensure it is communicated to, understood and adhered by employees (Bulgurcu et al., 2010)
Security Education, Training and Awareness	• Covers three elements: education, training and awareness to provide employees with knowledge, skills and alertness respectively • Plays a key role in employees' information security compliance behaviour (Bulgurcu et al., 2010) • Improves employees' behaviour, and enable organisations to hold employees accountable for their actions (Whitman & Mattord, 2008) • Increases employees' perceptions of vulnerability and severity of information security threats although they do not experience any security incidents (Workman & Gathegi, 2007) • Ensures employees understand their information security responsibilities, organisational policies and proper use of IT resources entrusted to them (NIST, 2003) • Minimizes accidental security breaches (CSI, 2009; Herath & Rao, 2009; Smith & Toppel, 2009; Whitman & Mattord, 2008)	• SETA is a continuous task and organisations must think of innovative ways to keep employees aware and alert of their responsibility to protect organisational information (von Solms & von Solms, 2009) • It requires support from the management and participation from everyone in the organisation • May require more resources to promote awareness through security talks, and security reminders printed on newsletters, security posters, mouse pads and mugs, or published on corporate websites
Preventive Security Systems	• Allows organisations to encrypt their confidential information, implement access controls to classified information and, monitor and block employee	• If the preventive systems restrict the use of OSN using corporate networks, employees can still use personal devices to access OSN sites

	postings on OSN (McAfee, 2010; Proofpoint, 2009) • Able to restrict the use of chat functions and third party applications and can be configured to designate some parts of the site off-limits (Messmer, 2009).	• May be able to restrict access to corporate networks but unable to change human behaviour (Smith & Toppel, 2009; von Solms & von Solms, 2009) • Computer-savvy employees are less deterred by preventive security systems since they can 'cheat' their way through the system (D'Arcy & Hovav, 2009) • The preventive security systems can be very costly (Messmer, 2009)

Table 2: Advantages and disadvantages of key deterrents to insider threats

However, which one of these control mechanisms is the most suitable approach to mitigate information leakage through OSN by employees? As mentioned previously, an organisation may have a security policy to limit the use of social media during working hours, and to implement this, it utilises a preventive security systems to automatically block access to these sites. However, the proliferation of OSN access using smartphones and other personal devices, allows sensitive information to be leaked, making security policy and preventive systems ineffective to prevent information leakage through this channel.

Furthermore, whilst APT attacks may be stopped by technological defence, the threats coming from direct actions of people, particularly the actions of compromised or vulnerable insiders are less suitable for software defences. As Smith & Toppel (2009, p.65) points out, since "APT attackers use valid user credentials and are able to log on to a network as any trusted employee would, relying on network perimeter defences is no longer effective". Therefore, organisations should focus on the human factor, on security awareness (Smith & Toppel, 2009). This again shows that preventive security systems are ineffective to address this issue.

Hence, we propose the implementation of information security education, training and awareness (SETA), as the guideline for organisations to address this issue since, as stated in Table 2, SETA plays a key role in employees' compliance behaviour (Bulgurcu et al., 2010) compared to ISP and technical controls.

According to Whitman and Mattord (2008), the rationale behind SETA is to improve organisational information security by:

- building in-depth knowledge to design, implement, or operate security programs for organisations and systems through security education for employees with information security responsibilities,
- developing employees' skills to perform their jobs while using IS more securely through security training, and
- improving employees' awareness to protect IS resources through security awareness programs.

Previously, we stated that DTPB theoretical model provides the underlying factors which drive employees' behaviour are the determinants of the behavioural intention. These factors are; the attitude of employees towards OSN use, social influence from peers and superiors, and perceived behavioural control that is determined by self-efficacy and facilitating conditions. Below we show how SETA can tackle this issue by addressing these factors.

Using SETA to address OSN behaviour

As stated earlier, the attitude towards social networking behaviour is based on the perceived ease of use and usefulness, and compatibility. As McKenna (2009, p. 19) pointed out **"**The problem is that it is so easy. Social networking sites ask you 'what are you doing now?' and you respond". Therefore, organisations should implement SETA programs to alert employees about the ease of social media use may result to the difficulty of controlling sensitive information appearing on these sites. Organisations should make their employees aware that once information is posted, it is almost impossible to control the flow of information because it is as easy for anyone to copy and distribute the information to other people, including APT attackers. We suggest that organisations should design a comprehensive SETA program that includes guidelines on the safe and secure use of social media in terms of accepting friends' requests, updating status, uploading photos and videos, clicking on links and using applications. The implications of these activities on APT attacks should also be explained.

With regard to subjective norms or social influence, organisations need to make it mandatory for all employees regardless of levels and positions to attend the awareness training sessions on the acceptable use of OSN sites and its impacts on organisational information security. An organisation wide SETA is vital to ensure employees understand their

information security responsibilities, organisational policies and proper use of IT resources entrusted to them (NIST, 2003). Additionally, all employees should also be informed about APT techniques and how APT can happen through the reconnaissance of targeted employees and organisations via this channel.

Similar to other insider threats, this problem is perceived to be more accidental than intentional especially due to pervasive use of mobile devices to access OSN sites. Concurring with Whitman & Mattord (2008), we propose SETA as the effective control mechanism to minimise accidental security breaches. Therefore, organisations should provide security education for staff with security responsibilities to design security awareness programs that inform all employees about the careless use of social media that could lead to damages to the organisation. The awareness will result to more mindful OSN behaviour while posting status updates, accepting friends' request, using applications and clicking on links. It is also imperative for the organisation to clearly state the repercussions of this problem to the organisation as well as to the employees. Make it clear to them that, targeted attacks on the organisation can cause great financial damages which can cause employees to lose their jobs. This understanding of the consequences for their actions should be able to prevent accidental leakage of information through this channel.

Based on these underlying factors of employees leaking information via OSN that subsequently maximises the chance of APT attacks, we concur that

> ***"Employees must understand the methods used by the attackers to gather information about a company and themselves. Understanding the tactics used allows them to recognise those situations where they are at risk so that they can change their behaviour and also know when and how to report suspected incidents." (Smith & Toppel, 2009, p.65).***

With this notion, we recommend that organisations should provide employees with information security responsibilities in-depth knowledge on OSN, APT and their impacts to organisations in order to design, implement and operate a comprehensive SETA program. Organisations should also develop skills for employees to securely engage in social networking by understanding how APT attacks can occur through social media use and instil awareness among their employees to protect personal and organisational information through awareness programs on OSN and APT. Furthermore, organisations need to review and monitor the SETA program to suit the changing computing environment periodically to ensure current information on information security threats are being communicated to employees.

The approach to understand human behaviour in order to address the behaviour that leads to security problems is an area worth researching since it defies traditional convention of information security solutions through technical approach. We acknowledge that information security policy and preventive security systems are also able to address this problem, thus, we suggest that more research in this area is required focusing on behavioural facets of information security, prior to confirming that SETA is the better solution to this problem.

CONCLUSION

Disclosed information on social media will not only tarnish organisation's reputation, but also invite other avenues of cybercriminals' attacks on organisations particularly APT that can cause serious financial damage. The ubiquitous nature of OSN, owing to the available smartphones and other mobile devices, shows that it is becoming a challenging channel of information leakage that is difficult to be controlled by organisations. The frequent and constant visits to these sites and social networking activities result to massive disclosure of information about employees and their work-related information, thus putting themselves and organisations as the target of cybercriminals.

Cybercriminals are currently no longer interested to take down organisations' networks as notorious acts but they are more financially motivated to steal valuable information from a targeted organisation. They do this through the weakest link in the organisation by gathering information of the employees on OSN sites, prior to launching spear phishing and social engineering attacks to obtain employees' credentials to ensure undetectable and longer access to the organisation's network. APT attackers do this by tricking employees into clicking on a link or using applications on social media to install Trojans or backdoor connected to a remote command-and-control server that collects organisational intellectual property. Furthermore, APT attackers are able to do reconnaissance on targeted organisations not only through explicit leakage of information but also by deducing any work-related information that is inadvertently leaked by employees. The seemingly insensitive information can be gathered and deduced to make up enough information to gain access credentials.

This conceptual study explores social media as the most challenging information leakage channel and its link to APT attacks. It explains how this phenomenon happens through the understanding of the underlying factors of information leakage via OSN that facilitates the suggestion to combat this problem. Since this threat is due to the actions of

employees, we suggest more research in this behaviour-changing approach; through the comprehensive design and implementation of SETA in organisations. This study offers contributions to research and practice by addressing the gaps concerning the behavioural aspects of information security and OSN security impacts on organisations. It is also perceived as timely and important considering the current media attention to this phenomenon.

REFERENCES

Ahmad, A., Ruighaver, A. B., & Teo, W. T. (2005, 21-24 Nov. 2005). An Information-Centric Approach to Data Security in Organisations. Paper presented at the TENCON 2005 2005 IEEE Region 10.

Ajzen, I. (1991). The Theory of Planned Behaviour. Organisational Behaviour and Human Decision Process, 50(2), 179-211.

BBC. (2010). Israeli military 'unfriends' soldier after Facebook leak. Retrieved 9 March 2010, from http://news.bbc.co.uk/2/hi/middle_east/8549099.stm

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness. MIS Quarterly, 34(3), 523-548.

Carvalho, V., Balasubramanyan, R., & Cohen, W. (2009). Information Leaks and Suggestions: A Case Study using Mozilla Thunderbird. Paper presented at the CEAS 2009 - Sixth Conference on Email and Anti-Spam.

Christofides, E., Muise, A., & Desmarais, S. (2009). Information Disclosure and Control on Facebook: Are They Two Sides of the Same Coin or Two Different Processes? Cyberpsychology and Behaviour, 12(3).
CISCO (2008). Data Leakage Worldwide: Common Risks and Mistakes Employees Make. Journal,

Colwill, C. (2010). Human factors in information security: The insider threat - Who can you trust these days? Information Security Technical Report, in press.

CSI. (2009). 14th Annual CSI Computer Crime and Security Survey: Executive Summary. New York: Computer Security Institute.

D'Arcy, J., & Hovav, A. (2009). Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. Journal of Business Ethics, 89, 59-71.

Everett, C. (2010). Social media: opportunity or risk? Computer Fraud & Security, 8-10.

Facebook. (2010). Facebook Statistics. Retrieved 14 Sept 2010, from http://www.facebook.com/press/info.php?statistics

Gaudin, S. (2009). Execs Worry That Facebook, Twitter Use Could Lead to Data Leaks. ComputerWorld Retrieved 2 June 2010, from http://www.computerworld.com/s/article/9136465/Execs_worry_that_Facebook_Twitter_use_could_lead_to_data_leaks

Goodchild, J. (2010). Social Media Risks: The Basics. CSO Security and Risk.

Grabosky, P., Smith, R. G., & Dempsey, G. (2001). Electronic Theft: Unlawful acquisition in cyberspace. Cambridge, U.K.: Cambridge University Press.

Gross, R., & Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks (The Facebook case). Paper presented at the ACM Workshop on Privacy in the Electronic Society (WPES), 2005, Virginia, USA.

Gudaitis, T. (2010). The Impact of Social Media on Corporate Security: What Every Company Needs to Know: Cyveillance, Inc.

Herath, T., & Rao, H. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18, 106-125.

ISO/IEC (2005). Information technology - Security techniques - Code of practice for information security management, ISO/IEC 17799:2005(E)

Jacobsson, S. (2010). Social Networks May Be Sharing Your Info with Advertisers. PC World.

Jansen, J. (2010). Strategic information disclosure and competition for an omperfictly protected innovation. The Journal of Industrial Economics, 58(2), 349-372.

Leitch, S., & Warren, M. (2009). Security issues challenging Facebook. Paper presented at the 7th Australian Information Security Management Conference, Perth, Western Australia.

Mansfield, R. (2010). UK MoD Secrets Leaked Onto The Internet. Retrieved January 25, 2010, from http://news.sky.com/skynews/Home/UK-News/Ministry-of-Defence-Staff-Have-Leaked-Secret-Information-16-Times-Onto-Social-Networking-Sites/Article/201001415535304

McAfee. (2010). Protecting Your Critical Assets: Lessons Learned from "Operation Aurora": McAfee, Inc.

Messmer, E. (2009). Fidelis spies data leakage via social networking sites. Network World.

Ng, V. (2009). US Congressman twitters secret trip to Iraq. Search Security Asia.

NIST. (2003). Building an Information Technology Security Awareness and Training Program. Maryland, U.S.: National Institute of Standards and Technology.

Paul, I. (2010). The Facebook data torrent debacle: Q&A. PCWorld.

Proofpoint. (2009). Outbound Email and Data Loss Prevention in Today's Enterprise. California.

Ristenpart, T., Tromer, E., Shacham, H., & Savage, S. (2009). Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. Paper presented at the Conference on Computer and Communications Security.

Rose, S., Chandramouli, R., & Nakassis, A. (2009). Information Leakage Through the Domain Name System. Paper presented at the Cybersecurity Applications & Technology Conference For Homeland Security.

Smith, A. M., & Toppel, N. Y. (2009). Case study: Using security awareness to combat the advanced persistent threat. Paper presented at the 13th Colloquium for Information Systems Security Education (CISSE), University of Alaska, Fairbanks, Seattle.

Sophos. (2010). Security Threat Report: 2010. Boston, Massachusetts: Sophos Group.

Spinney, M. (2010). Identity & Privacy in Social Media. Michigan, U.S.: Ponemon Institute.

Straub, D. (1990). Effective IS Security. Information Systems Research, 1(3), 255-276.

Stutzman, F. (2006). An evaluation of identity sharing behaviour in social network communities. International Digital Media and Arts Association 3(1), 10-18.

Symantec. (2010). Symantec Global Internet Security Threat Report: Trends for 2009. California, U.S.: Symantec Corporation.

Taylor, S., & Todd, P. (1995). Understanding information technology usage: A test of competing models. Information Systems Research, 6(2), 144-176.

Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The insider threat to information systems and the effectiveness of ISO17799. Computers & Society 24, 472-484.

Verizon, & USSS. (2010). Data breach investigations report: A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service: Verizon.

von Solms, S. H., & von Solms, R. (2009). Information Security Education, Training and Awareness. In S. H. von Solms & R. von Solms (Eds.), Information Security Governance (pp. 113-126). New York: Springer.

Warwick, G. (2010). Future of Cyber - Staying Ahead. Aviation Week & Space Technology, 172.

Westervelt, R. (2009). Botnet masters turn to Google, social networks to avoid detection. Retrieved 28 January 2010, from http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1373974,00.html

Whitman, M. E., & Mattord, H. J. (2008). Principles of information security. Stamford, Connecticut: Course Technology.

Workman, M., & Gathegi, J. (2007). Punishment and ethics deterrents: A study of insider security contravention. Journal of the American Society for Information Science and Technology, 58(2), 212-222.

Young, K. (2010). Policies and procedures to manage employee Internet abuse. Computers in Human Behaviour, 26, 1467-1471.

Zetter, K. (2010). Report Details Hacks Targeting Google, Others. Wired.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers for their helpful comments. Nurul Nuha Abdul Molok's PhD research is financed by the Malaysian Ministry of Higher Education and International Islamic University Malaysia.