Online Social Networking: A Source of Intelligence for Advanced Persistent Threats

Nurul Nuha Abdul Molok, Department of Information Systems, The University of Melbourne, Melbourne, VIC, Australia

Atif Ahmad, Department of Information Systems, The University of Melbourne, Melbourne, VIC, Australia

Shanton Chang, Department of Information Systems, The University of Melbourne, Melbourne, VIC, Australia

ABSTRACT

The professionalization of computer crime has resulted in a shift in motivation away from bragging rights towards financial gain. As a result, the operational tactics of cyber criminals is beginning to incorporate reconnaissance and intelligence gathering to inform attack planning. This paper discusses why information leakage in general, and Online Social Networking (OSN) in particular, has become a source of intelligence for attackers. Further, the paper profiles a range of security measures available to organizations to combat information leakage through OSN and identifies future directions for research into security culture and behaviour change.

Keywords: Advanced Persistent Threats, Cyber Espionage, Information Leakage, Information Security, Online Social Networking (OSN), Social Media

INTRODUCTION

Modern organizations are exposed to a wide range of information security risks resulting in loss, modification or disclosure of information and damage to underlying information infrastructure. Although much of this can be traced to the (frequently accidental but sometimes deliberate) actions of insiders, malware infections and system penetration by external malicious 'hackers' remain a key instigator (CSI, 2009).

The clear and present danger posed by external malicious hackers is not surprising. In fact the spectre of young males wielding considerable power through the digital environment against relatively powerless corporations has long remained in the public psyche. Perhaps this can be attributed to aging films like 'WarGames' where an unsuspecting teenager engages in simulated thermonuclear warfare when he discovers he can connect to military computers through the public telephone system. The 1983 film was believed to influence the rise of computer hacking in the 1980s (Leeson & Coyne, 2005).

DOI: 10.4018/ijcwt.2012010101

However, what is particularly misleading about the perception of hacker attacks is that they continue to be motivated by a sense of adventure. This is not the case, this paper will argue that a clear trend towards professionalization of computer crime is emerging indicating that previous motivations have been replaced by that of financial gain.

The rise of online social networking (OSN) and its pervasive use among employees have been reported to be beneficial but at the same time detrimental to organizations. Despite its benefits to organizations in terms of advertising products and services, gathering consumer feedbacks, and making employment decisions (to name a few), it is capable of jeopardizing organizational information security. It has become an avenue for cyber espionage, malware attacks, bandwidth strain and productivity issues among employees (Abdul Molok, Ahmad, & Chang, 2011). People share a lot of information about themselves with their friends and family on OSN sites, without realizing the information can also be leaked to the enemies. The ubiquitous nature of these sites has turned social media into a potential platform for gathering information and doing surveillance on targets.

In this paper, we discuss the impact of the change of motivation on operational tactics and argue that modern hackers target individual organizations after considerable intelligence gathering and surveillance which is primarily targeted at profiling insiders that have the authority and/or knowledge critical to success of the hacker attack. The paper further argues that this reality puts the phenomenon of (OSN) in a new light as it presents a rich source of intelligence on topics of particular interest to the attackers. And finally, the paper considers approaches to mitigating the problem of information leakage through OSN which culminates in a series of research questions that charts future research directions.

SHIFTING TRENDS IN THE THREAT LANDSCAPE

Leeson & Coyne (2005) cite a number of papers (Blake, 1994; Sterling, 1991; Taylor, 1999; Thomas, 2002) that suggest fame or peer recognition as the primary reason for hacking. The following quote from Bruce Sterling's hacker classic "The Hacker Crackdown: Law and Disorder on the Electronic Frontier" makes this point (Sterling, 1991):

> *Hackers can be shy, even reclusive, but when they do talk, hackers tend to brag, boast and strut. Almost everything hackers do is INVISIBLE [sic]; if they don't brag, boast, and strut about it, then NOBODY WILL EVER KNOW [sic]. If you don't have something to brag, boast, and strut about, then nobody in the underground will recognize you and favor you with vital cooperation and respect. The way to win a solid reputation in the underground is by telling other hackers things that could only have been learned by exceptional cunning and stealth… Hackers hoard this knowledge, and dwell upon it obsessively, and refine it, and bargain with it, and talk and talk about it.*

However, in the last five years, a clear shift in the motivation of attacks towards financial gain and away from 'bragging rights' has become apparent (CSI, 2007; Gartner, 2006). The annual Computer Security Institute (CSI) survey reported the following in its 2007 edition:

> *…security professionals observing the state of the "hacker" underworld have long been very concerned about several significant factors likely to change the face of cybercrime within organizations. The first of these is the shift toward a "professionalization" of computer crime. …Suffice it to say, though, that more*

of the perpetrators of current computer crime are motivated by money, not bragging rights. (CSI 2007, p.16)

CSI (2007) and Gartner (2006) agree that cyber exploits are not predominantly aimed at getting in the paper. Further, cyber criminals are now seeking alliance with more traditional forms of organized crime (Blitstein, 2007). Such alliances might prove to be useful in feeding intelligence to hackers on which targeted employees in organizations have a vulnerability that can be exploited (gambling addiction, etc.).

Perhaps, the shift in the motivation towards financial gain can be further demonstrated with the increased incidents of financial fraud cases from 12% in 2008 to 20% n 2009 (CSI, 2009). The more recent CSI Survey 2010/2011 reported that security breaches mostly occur in financial institutions and organizations are concerned with *"stealthier forms of data exfiltration with newer, complex attacks"* (CSI, 2010, p.2).

APT OPERATIONAL MODEL OF ATTACK

The trend of motivation for information security attacks towards financial gain implies that cybercriminals are now turning to 'high value' targets rather than random or generalized network attacks as in the past. Previously hackers engaged in 'shot gun' style attacks – where the objective was to probe a large number of network addresses for opportunities for exploitation followed by trespass and exploitation of computer networks for the 'thrill of the hunt' and subsequent 'bragging rights'. The change in motivation implies hackers are now targeting individual organizations for financial gain which necessitates a consequential change in operational tactics (Gartner 2006, p2).

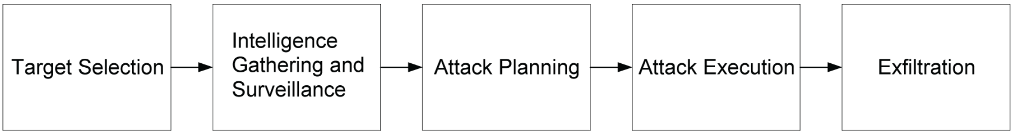
Financially motivated attacks are usually targeted, aiming at specific industries, specific companies and specific types of information within those companies. The techniques used by attackers are stealthier, trying to evade detection rather than cause noisy denial-of-service attacks and using techniques to cover their tracks by deleting or modifying audit trails. Such attacks are more complex and will often consist of several stages of reconnaissance, preliminary exploitation and then deeper exploitation that consists of implanting malicious executables.

Criteria for target selection revolves around financial gain, and intelligence is collected and surveillance is undertaken to analyze the defenses of the organization before a tailored attack is planned and executed (see Figure 1) to exploit the specific vulnerabilities of the target organization.

Interestingly, the term 'Advanced Persistent Threat' (APT) was coined by the United States Air Force in 2006 (Martin, 2011). It has been used to describe a well-funded and well-organized attack that is financially-motivated and employs stealthy techniques such as zero-day exploits to breach organizational defenses and to establish a long-term occupying force inside an organization's perimeter (Martin, 2011; Smith & Toppel, 2009).

The second phase of attack in the model above, namely 'Intelligence Gathering and Surveillance' is of particular interest. Examining what literature says about APT tactics in this

Figure 1. Traditional attack phases (adapted from Ahmad et al (2004))



phase reveals that reconnaissance and information gathering occurs on targeted organizations through identified employees (Smith & Toppel, 2009). It stands to reason that attackers will be trying to determine where the information asset or function is in the organization and which employees have the necessary credentials and/or access to facilitate their objectives. Interestingly, the kinds of information required to determine the usefulness of an employee may not be sensitive at all. Information about social networks, job functions, important events, and personal vulnerabilities is useful. Attackers tend to target employees who are vulnerable; disgruntled employees, employees with financial problems or with weaknesses such as gambling, pornography and drug dependence, who can be induced or coerced into cooperation. Once APT attackers have identified the employees, they may use social engineering techniques to obtain valid user credentials. These credentials can be used in a spear-phishing message that appears legitimate tricking employees into divulging sensitive information or clicking on a link or attachment that contains malicious code.

APT attackers tend to target financial, government and defence sectors, however, recently large organizations are becoming the target. In January 2010, the media reported that Google, Adobe and other large U.S. organizations 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).

SOURCES OF INTELLIGENCE WITHIN ORGANIZATIONS

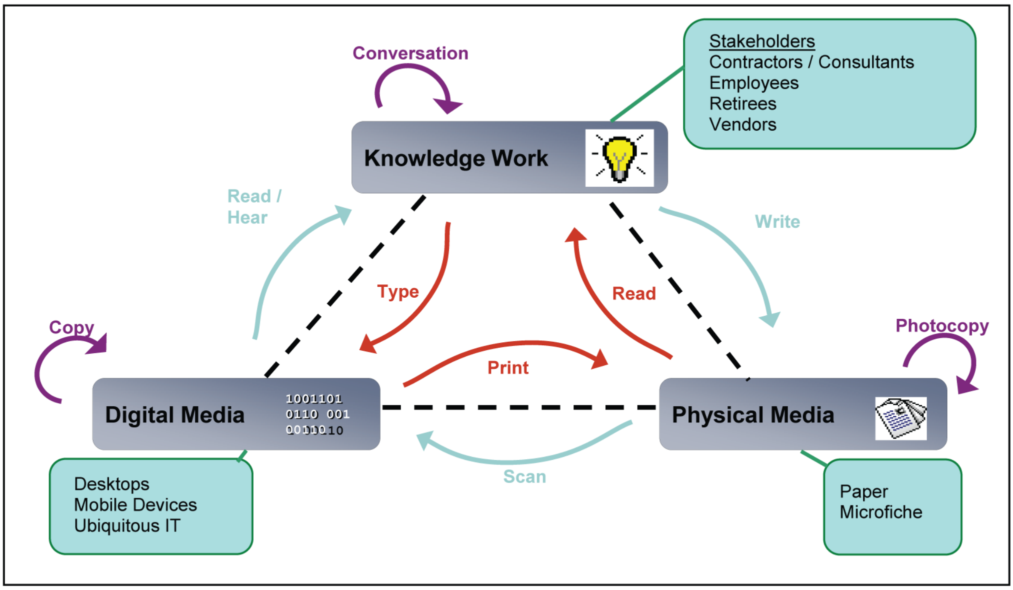
It is apparent that APT attacks rely on intelligence collected about the organization to identify which employees to target based on their authority in the organization, the tasks they are working on or have worked on in the past, and their vulnerabilities. From an organizational perspective the challenge of denying such information to APT attackers is a difficult one.

Leakage of information (and knowledge) in organizations has been recognized in literature and practice as a significant security concern (Ahmad, Ruighaver, & Teo, 2005; Bhattacharya & Guriev, 2006; Winkler, 2007; Yayla & Hu, 2011). For example, Yayla and Hu (2011) point out that the leakage of organizational knowledge may result in tangible and intangible losses to the organization including competitive advantage, productivity, and trust with existing clientele. The most recent Global Security Survey conducted by Ernst & Young titled "Borderless Security" reported that *"64% of respondents indicated that data (i.e. disclosure of sensitive data) was one of their top five areas of IT risk"* (Ernst & Young, 2010).

Sensitive information frequently exists on hardcopy and softcopy media as well as in the knowledge of personnel (Ahmad et al., 2005). Copies of such information are usually not inventoried or monitored and can proliferate unchecked across the organization. Literature points to a number of channels of leakage in organizations; face-to-face conversation and printing facilities, email, cloud computing, domain name systems, portable data devices and OSN (Abdul Molok, Ahmad, & Chang, 2010).

The model in Figure 2 shows information tends to exist in one of two states – 'resident' or 'transmitted'. The term 'resident' implies the information is not moving and is therefore stored in an information 'container'. There are three categories of containers – hardcopy containers (such as paper and microfiche), softcopy containers (such as USB sticks and hard disks), and cognitive containers (the minds of employees which is illustrated in Figure 2 as 'knowledge work'). When information is transmitted it takes on one of the nine information flows identified in the figure. From a security perspective it is interesting to note that security strategies should not be exclusively focused on protecting knowl-

Figure 2. Knowledge leakage model (Ahmad et al., 2005)



edge in the digital environment whilst neglecting the same knowledge when it exists on paper or among employees. From the perspective of an attacker targeting particular information or knowledge it doesn't matter where it comes from (i.e. which container or information flow leaked the information). Information security strategy should be information-centric rather than state-centric, container-centric or flow-centric (Winkler, 2007).

Information can leak from any container or transmission path thereby making it difficult for organizations to control the many categories of information in the organization. Further, from the perspective of the APT attacker, information is best collected in a cost-efficient way. Since organizations tend to focus their information security strategy around containers (such as in the digital environment rather than on physical media such as paper) it may be easier simply to focus on the conversations between employees rather than to hack the network and trawl through the volumes of data in storage looking for the information required.

ONLINE SOCIAL NETWORKING

OSN is the new socialization tool in the digital age (Young, 2009) which consists of social networks (Facebook, LinkedIn and MySpace), microblogging (Twitter), content communities (YouTube and Flickr), blogs, wikis and forums (Mayfield, 2008). Although OSN is often epitomised by sites like Facebook, LinkedIn, MySpace and Twitter (Wilson, 2009; Young, 2009), the paper focuses on OSN behaviour regardless of the types of OSN media. Hence, OSN in this context is referred to the practice of sharing information and contents on *"online social media which share most or all of the following characteristics: participation, openness, conversation, community and connectedness"* (Mayfield, 2008, p.5).

The evolution of social networking was discussed in great length by Boyd and Ellison (2007). They defined social network sites as *"web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list* *of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."* (Boyd & Ellison, 2007, p.2). Based on this definition, SixDegrees.com was recognized as the first social network that was initiated in 1997 for people to connect with friends and send messages to each other (Boyd & Ellison, 2007). On the other hand, Gross and Acquisti (2005) reported that the social networking concept was introduced in 1960s but its growth and commercial interest were contributed by the Internet advancement. The purpose and patterns of use differ from one site to another within these categories; business, common interests, dating, friends, pets and photos (Gross & Acquisti, 2005).

Statistics show that the Internet activities globally are taking place on OSN. To date, OSN monopolizes the Global Top 10 Internet traffic analysis with Facebook at number two, followed by YouTube, Wikipedia, Blogspot, and Twitter (Alexa, 2011). Currently, there are more than 800 million active users on Facebook and 50% of them access Facebook daily including 350 million users who access the site through mobile devices (Facebook, 2011). Our previous work showed that employees use Facebook at workplace, home and anywhere, using mobile devices, thus blurring the boundary between work and home life resulting to sharing of business and personal information on this site (Abdul Molok et al., 2011). Indeed, OSN sites particularly Facebook, have become the global phenomenon nowadays, raising information security problems to the organizations and privacy issues to the individuals (Sophos, 2010).

Among popular OSN sites, Facebook is viewed to be the site that poses the biggest risk to security (61%), significantly ahead of MySpace (18%), Twitter (17%) and LinkedIn (4%) (Sophos, 2010). Many organizations are concerned with OSN since they can affect productivity, information leakage among employees, malware and phishing attacks, and provides capabilities for cybercriminals to gain more access to corporate servers through reconnaissance on employees' OSN sites (Gudaitis, 2010; Smith & Toppel, 2009; Sophos, 2010; Symantec, 2010; Wilson, 2009).

OSN: A Useful Channel of Intelligence for APT

Among the channels of leakage, we suggest that (OSN) is particularly significant for a number of reasons. It creates an avenue for cybercriminals to do surveillance and gather intelligence, sabotage organizations' networks and utilize corporate resources to launch attacks (Colwill, 2010; Gudaitis, 2010; Leitch & Warren, 2009). It is also difficult for organizations to control the flow of information disclosed on these sites, since the information can be instantaneously reached by wider audience from anywhere at any time.

The use of social media allows APT to profile employees since they are likely to post 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 do not need to be explicit private organizational 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 organizations.

Private information on targeted employees can also be gathered through their users' profiles even if the strictest privacy settings had been set (Steel & Fowler, 2010). Unsurprisingly, 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 organizations to realize their attacks.

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"*.

Typical OSN sites have 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 capabilities as attack vectors through its available functionalities.

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). Furthermore, since many users engage in social networking during their internet activities daily routine, these sites become a key source of intelligence by which threat agents can launch targeted attacks on organizations and individuals by using spam, 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

Table 1. OSN functions and potential problems to organizations

OSN Functionalities	Potential Security Problems	Impacts to Organizations
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 APT to obtain confidential information about organizations.
Friends' Requests	Carelessness in accepting friends' requests could result to adding 'enemies' instead of 'friends' who have more access to users' information.	Masquerading as 'friends' allows APT to monitor activities of employees' within organizations thus allowing them to obtain employee credentials for future exploits on 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 organizations.	Sensitive photos and videos may cause embarrassment to the organization as well as employees allowing APT blackmailing opportunities.
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 APT to sabotage corporate networks, to monitor and access corporate assets and steal intellectual property.

challenging channel of information leakage due to the difficulty of managing organizational information that is disclosed through employees' sites.

Although academic literature seldom discusses the information security impacts of OSN on organizations, social networking sites especially Facebook and Twitter have made the headlines since 2009 (Goodchild, 2010). Concerns regarding OSN as an avenue for security threats is supported by prominent security surveys. For example, the 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 organization and its employees (Symantec, 2010). Further, 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, organizations were concerned about their employees engaging in OSN because it wasted organizational time and drain the bandwidth. Now, although productivity is still a concern, organizations are becoming more worried about their confidential information being leaked through employees' social networking activities (Gaudin, 2009; Sophos, 2010).

MITIGATING INFORMATION LEAKAGE THROUGH OSN: AN ORGANIZATIONAL CHALLENGE

Since information leakage through employees' social networking activities provides a key avenue for APT attacks, it is essential for organizations to address employees' behaviour that leads to this problem. This section investigates the safeguarding measures for organizations to mitigate this problem.

Controlling information disclosure on OSN is about influencing the decision-making behavior of employees. IS security literature proposes information security policy (ISP), security education, training and awareness (SETA) and access control as a means of maintaining a security environment (Bulgurcu, Cavusoglu, & Benbasat, 2010; Straub, 1990; Theoharidou, Kokolakis, Karyda, & Kiountouzis, 2005; Workman & Gathegi, 2007). Table 2 below shows how these control mechanisms can help organizations to deter employees from leaking information through OSN.

An organization may have a security policy to limit the use of social media during working hours. Implementation may utilize preventive security systems to automatically block access to such sites. However, the proliferation of OSN access using smart phones and other personal devices, allows sensitive information to be leaked circumventing security policy and preventive systems.

Furthermore, whilst externally based conventional attacks may be stopped by technological defences (firewall perimeter, intrusion detection and access control), the threats coming from direct actions of compromised yet authorized insiders are less suitable for software defences. As Smith & Toppel (2009, p.65) point 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"*.

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

Control Mechanisms	Potential Advantages	Potential Disadvantages and Issues
Information Security Policy (ISP)	• clearly defines the classification of information for employees to understand the types of sensitive information, and how to handle them • specifies acceptable use of OSN sites and corporate assets to ensure confidentiality, integrity and availability of information • provides understandable security policies that are integrated with business processes and aligned with job requirements (CISCO, 2008)	• must be designed, implemented, enforced and reviewed to ensure effectiveness (ISO/IEC, 2005) • employee 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) • requires an awareness program to ensure policies are communicated, understood and adhered to by employees (Bulgurcu et al., 2010)
Security Education, Training and Awareness	• provides employees with knowledge, skills and alertness respectively • plays a key role in employees' information security compliance behaviour (Bulgurcu et al., 2010) • influences employee behaviour, allows employees to be held accountable for actions (Whitman & Mattord, 2008) • ensures employees understand their security responsibilities, 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)	• maintaining effectiveness requires innovative ways to keep employees aware and alert of their security responsibilities (von Solms & von Solms, 2009) • requires support from management and participation from everyone in the organization • 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 organizations to encrypt their confidential information, implement access controls to classified information and, monitor and block employee 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).	• employees can use personal devices to access OSN sites from home • may not change human behaviour (Smith & Toppel, 2009; von Solms & von Solms, 2009) • does not deter computer-savvy employees since they can 'cheat' their way through the system (D'Arcy & Hovav, 2009) • can be very costly (Messmer, 2009)

Using SETA to Address OSN Behaviour

The study by Abdul Molok et al. (2010) investigates the underlying factors that cause risky use of OSN among employees that contributes to information leakage. They suggest that organizations can mitigate this problem by tackling the root causes of the problem; by changing employees' attitude towards OSN use, increasing superior's influence and decreasing peer influence through acceptable social media use policies, and, controlling employees' OSN activities using available facilitating conditions. These strategies should be incorporated into an organization-wide education, training and awareness on information security and OSN.

From the discussion on APT tactics in the Intelligence Gathering and Surveillance phase, some observations can be made that relate to the SETA program. Firstly, the SETA program must be designed to influence the behaviour of employees on OSN. This may require imparting each employee with a working (in-depth) knowledge of information security responsibilities. Employees must be aware how APT attacks occur through social media.

The SETA program must be complemented by a clear understanding of the sensitivity of various types of information. This requires a classification scheme to be applied to the various data sets in circulation in the organization. Furthermore, organizations may 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. Guidelines on the safe and secure use of social media in terms of accepting friends' requests, updating status, uploading photos and videos, and clicking on links and using applications must be part of the program.

The information security industry recommends an integrated approach; an overall Web 2.0 threats management system by combining ISP, preventive systems and SETA (Gudaitis, 2010; Sherry, 2010; Sophos, 2010; Symantec, 2010; Websense, 2010). IS security scholars posit that ISP is useful to minimize internal security breaches but recommend further studies on employees' attitude and beliefs to enhance compliance to the policies (Bulgurcu et al., 2010; Herath & Rao, 2009). D'Arcy and Hovav (2009) suggest organizations need to consider different control mechanisms for different groups of employees based on the evidence that computer savvy employees are less deterred by SETA and preventive security systems. Indeed there is no one size fits all solution to this problem.

PREVENTING LEAKAGE THROUGH OSN: FUTURE RESEARCH

As mentioned in the Online Social Networking section, the use of social media is so ubiquitous that to control such use and the disclosure of information on these sites poses a unique challenge for any organizations seeking to minimize information leakage among employees. This paper shows that relying on a purely technical approach to security is no longer viable with APT attacks since the attack may be facilitated by compromised insiders with security clearance. However, more research is needed to derive specific guidelines on addressing APT attacks. There are three facets to this problem. Firstly, the precise nature of the attack must be examined before disruption strategies can be devised. Secondly, risky behaviour of employees that lead to information leakage must be profiled to assist in developing strategies towards behaviour change. Thirdly, a more systematic and comprehensive approach to the protection of sensitive information is required. Thus, we propose that the following questions require further research:

1. How are APT attacks on targeted organizations realized through the use of OSN sites?
2. Why do employees engage in risky OSN use that could lead to leakage of organizational information?
3. How can organizations safeguard their information from being leaked by employees through OSN?

Perhaps the most challenging aspect of educating employees is awareness of 'context'. For information to be protected during OSN, employees must make decisions whether or not to disclose particular information because of its sensitivities. But sensitivity is largely influenced by context. For example, consider once again the case where the wife of the chief of MI6 disclosed that her husband would attend a social gathering at particular location at a particular time. The disclosure may not have appeared to be harmful given the context within which it took place. However, in a national security context the same information adopted a different level of sensitivity. This phenomenon highlights the difficulty for employees in considering the potential value that a piece of information may have outside of the context of their OSN conversation. In fact it may well be that employees may not be aware of the significance of some of the knowledge or information they may have.

This is one important reason why the SETA program must consider assisting employees to self-assess the significance of what they know and the responsibilities that come with that knowledge.

CONCLUSION

The proliferation of Web 2.0 technologies especially online social media coincides with a paradigm shift in the security threat landscape. Cyber criminals are engaging in intelligence gathering and surveillance towards targeting 'high value' organizations for financial gain. Thus, their operational tactics are becoming more sophisticated using modern blended social engineering and zero-day attacks. This advanced persistent threat or APT can extract useful intelligence from OSN to profile employees who have information or authority that can be exploited as part of the attack.

Conversations that were once private, short-lived and brief have become public, permanent and instantaneously accessible when disclosed on social media. Employees may potentially divulge information without recognizing the significance of their disclosure.

This study explores social media as the most challenging channel of information leakage, and the link to APT attacks. Since this threat is due to the actions of employees, we suggest more research into behaviour-change is needed through a comprehensive design and implementation of SETA in organizations.

REFERENCES

Abdul Molok, N. N., Ahmad, A., & Chang, S. (2010). Understanding the factors of information leakage through online social networking to safeguard organizational information. In *Proceedings of the 21st Australasian Conference on Information Systems (ACIS2010)*, Brisbane, Australia.

Abdul Molok, N. N., Ahmad, A., & Chang, S. (2011). Disclosure of organizational information by employees on Facebook: Looking at the potential for information security risks. In *Proceedings of the 22nd Australasian Conference on Information Systems (ACIS2011)*, Sydney, Australia.

Ahmad, A., Ruighaver, A. B., & Teo, W. T. (2005). An information-centric approach to data security in organizations. In *Proceedings of the TENCON 2005 2005 IEEE Region 10*.

Alexa. (2011). Alexa Top 500 Global Sites. *Alexa Internet, Inc.* Retrieved December 29, 2011, from http://www.alexa.com/topsites

Bhattacharya, S., & Guriev, S. (2006). Parents vs. trade secrets: Knowledge licensing and spillover. *Journal of the European Economic Association*, *4*(6), 1112–1147. doi:10.1162/JEEA.2006.4.6.1112.

Blake, R. (1994). *Hackers in the mist*. Chicago, IL: Northwestern University.

Blitstein, R. (2007). *San Jose police fight online crime*. Ghosts in the Browser.

Boyd, D., & Ellison, N. (2007). Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, *13*(1). doi:10.1111/j.1083-6101.2007.00393.x.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *Management Information Systems Quarterly*, *34*(3), 523–548.

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 & Behavior*, *12*(3). doi:10.1089/cpb.2008.0226 PMID:19250020.

CISCO. (2008). *Data leakage worldwide: Common risks and mistakes employees make*. San Jose, CA: CISCO Systems Inc..

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

CSI. (2007). *12th annual computer crime and security survey*. Orlando, FL: Computer Security Institute.

CSI. (2009). *14th annual CSI computer crime and security survey: Executive summary*. New York, NY: 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. doi:10.1007/s10551-008-9909-7.

Ernst, & Young. (2010). *Borderless security: Ernst & Young's 2010 global information security survey*: Ernst & Young Global Limited.

Facebook. (2011). *Facebook statistics*. Retrieved December 29, 2011, from http://www.facebook.com/press/info.php?statistics

Gartner. (2006). *Augment security processes to deal with the changing internet threat*: Gartner Inc.

Gaudin, S. (2009). Execs worry that Facebook, Twitter use could lead to data leaks. *ComputerWorld*. Retrieved June 2, 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.

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks (The Facebook case). In *Proceedings of the ACM Workshop on Privacy in the Electronic Society (WPES)*, Virginia.

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. doi:10.1057/ejis.2009.6.

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.

Leeson, P. T., & Coyne, C. J. (2005). The economics of computer hacking. *Journal of Law. Economic Policy*, *1*(3), 511–532.

Leitch, S., & Warren, M. (2009). Security issues challenging Facebook. In *Proceedings of the 7th Australian Information Security Management Conference,* Perth, Western Australia.

Martin, S. (2011). *Advanced persistent threats call for a reality check*. SC Magazine.

Mayfield, A. (2008). What is social media? Retrieved from http://www.icrossing.com/research/what-is-social-media.php

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.

NIST. (2003). *Building an information technology security awareness and training program*. Gaithersburg, MD: National Institute of Standards and Technology.

Proofpoint. (2009). *Outbound email and data loss prevention in today's enterprise*. California.

Sherry, D. (2010). *New web, new threats*. Information Security.

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

Sophos. (2010). *Security threat report: 2010*. Boston, MA: Sophos Group.

Spinney, M. (2010). *Identity & privacy in social media*. Traverse City, MI: Ponemon Institute.

Steel, E., & Fowler, G. (2010). Facebook in privacy breach: Top-ranked applications transmit personal IDs, a journal investigation finds. *The Wall Street Journal*. Retrieved from http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html

Sterling, B. (1991). *Cyber view 91 report*.

Straub, D. (1990). Effective IS security. *Information Systems Research*, *1*(3), 255–276. doi:10.1287/isre.1.3.255.

Stutzman, F. (2006). An evaluation of identity sharing behavior 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*. Mountain View, CA: Symantec Corporation.

Taylor, P. (1999). *Hackers: Crime in the digital sublime*. London, UK: Routledge. doi:10.4324/9780203201503.

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.

Thomas, D. (2002). *Hacker culture*. Minneapolis, MN: University of Minnesota Press.

Verizon, & USSS. (2010). *Data breach investigations report: A study conducted by the Verizon RISK Team in cooperation with the United States Secret Service*. New York, NY: 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, NY: Springer. doi:10.1007/978-0-387-79984-1_10.

Websense. (2010). *2010 threat report*. San Diego, CA: Websense, Inc.

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

Wilson, J. (2009). Social networking: The business case. *Engineering & Technology, June 2009,* 54-56.

Winkler, I. S. (2007). *Zen and the art of information security*. Rockland, MA: Syngress Publishing, Inc..

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. doi:10.1002/asi.20474.

Yayla, A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, *26*, 60–77. doi:10.1057/jit.2010.4.

Young, K. (2009). Online social networking: An Australian perspective. *International Journal of Emerging Technologies and Society*, *7*(1), 39–57.

Zetter, K. (2010). *Report details hacks targeting Google, others*. Retrieved August 18, 2010, from http://www.wired.com/threatlevel/2010/02/apt-hacks/#ixzz0ww3yJE4t

Nurul Nuha Abdul Molok is currently a PhD student at the Department of Information Systems, The University of Melbourne. She is also a lecturer at the International Islamic University Malaysia, under study leave. She holds a certificate in ISO27001:2005 Information Security Management Systems (ISMS) Lead Auditor from EQS Asia – UK Excel Partnership. She was a member of ISO/IEC JTC 1/SC 27/WG 1 "Information Security Management Systems", Information Security Technical Committee, Department of Standards Malaysia.

Atif Ahmad is an information security researcher and independent security consultant based at the Department of Information Systems, University of Melbourne. His research interests are in asymmetric warfare and information security risk assessments especially where knowledge artifacts are concerned. In previous years Atif has worked as a consultant for Pinkerton and WorleyParsons where he applied his expertise to Internet corporations and critical infrastructure installations. Atif is a Board Certified Protection Professional (CPP) with the American Society for Industrial Security and holds an adjunct position at the secau Security Research Centre at Edith Cowan University.

Shanton Chang is a Senior Lecturer in Change Management & Social Impacts of Information Systems at the Department of Information Systems, University of Melbourne. He received his PhD in Competencies for Managing Multicultural Workforces from the Monash University and is interested in organisational cultures and managing behavioural change. His current primary areas of research include the Social Aspects of Broadband Technology Adoption, Online Behaviour and Information Needs. He is particularly interested in the online behaviour of young people in the health, educational and business contexts.