Student Awareness of the Risks Associated with the Use of Mobile and Wireless Technologies and Applications

Maria Sagrario R. Simbulan
University of the Philippines in Diliman
Extension Program in Pampanga, Philippines

msrsimbulan@up.edu.ph

Abstract

This study looks at the online behavior of a hundred business management students and attempts to determine the respondents' awareness of the risks associated with the use of mobile technologies. Three questions were formulated for this study. First, when the respondents use mobile technologies, with whom do they communicate and for what purpose? The results showed that the respondents were comfortable with mobile computing and that mobile technologies were easily accessible to them. Mobile applications allowed them to complete tasks, to coordinate curricular and extra-curricular activities, and to communicate with teachers, both on a personal and a professional level. Second, what information do the respondents send or receive? Seventy-five or more of the respondents sent files and website links by email and by instant messaging. Third, are the respondents aware of the risks associated with the use of mobile technologies? Over half of the respondents were aware that using chat/IM or email without adequate safeguards could expose the school network to viruses, spyware or malware. Surprisingly, the respondents showed a lack of awareness of the potential risks that open, unsecured Bluetooth cellphone connections pose to the university's data and files. Some general recommendations are offered to help protect the institution's networks and IT infrastructure.

Keywords: mobile technology risks, student online behavior, chat/IM, email, SMS

Introduction

This research, based on a survey conducted in April 2009, focuses on evaluating the respondents' awareness of the risks associated with the use of mobile and wireless technology applications, particularly texting, email, chat, and instant messaging. The respondents are third- and fourth-year business management students studying in a state university. Specifically, the study attempts to address the following questions: When the respondents use mobile technologies, with whom do they communicate and for what purpose? What kinds of information do the respondents send or receive? Are the respondents aware of the risks associated with the use of mobile technologies to access the Worldwide Web and the Internet?

The use of mobile and wireless applications in the academe provides benefits to the students, to faculty members and to the academic institution itself. By enabling access to timely and accurate information, mobile and wireless applications give students the ability to communicate and interact with family members, friends, school administrators, teachers, communities, and the government at all levels at any time and from anywhere. Faculty members are able to interact with students even beyond class hours, to answer questions, provide research direction, or clarify instructions. Mobile communications also allows them to coordinate and communicate with colleagues and administrators on school-related matters. This ability to communicate and interact is one of the most significant benefits of using mobile technologies (Castleman, Harper, Herbst, Kies, Lane & Nagel, 2001).

Mobile and wireless technologies also provide faculty with more options and flexibility in terms of course content and delivery, allowing them to incorporate eLearning and online activities to enrich regular classroom-based instruction. The main benefits for school administrators are faster communications, better coordination, and increased capability to meet the demands of students and faculty for access to information to do research, fostering creativity in the academic setting (Qinyin, Davies, Grout & Cunningham, 2009).

When utilized correctly and with adequate safeguards in place, using mobile technologies in the academic setting can help create safe virtual communities (Päykkänen, Räisänen & Isomäki, 2006; Perry, O'Hara, Sellen, Brown &Harper, 2001) that allow students to collaborate on curricular and extra-curricular projects, share ideas and experiences with peers, and discuss issues with family, teachers and administrators. In many ways, utilized appropriately and with an understanding of the potential risks, using mobile and wireless technologies deliver major benefits to all who use these technologies. However, when misused or over-used, mobile technologies and applications in the academic setting can distract students from their schoolwork and add to school-related stress (Castleman et al., 2001; Waycott & Kukulska-Hulme, 2003; Xinhao, Wei & Min, 2008).

There are many risks relating to the use of mobile and wireless technologies in organizations. This research paper will focus on two specific risks that will have the most impact on an academic institution. The first risk is that proprietary and/or confidential information can be stolen from digital storage devices accessible through the University’s network then transferred to parties whose intentions are not in the best interest of the institution. Some examples of this confidential information are university entrance applications and enrollment records, student grades, examinations, proprietary ongoing and completed research data, and faculty information and performance evaluations.

The second risk is that digital files transmitted using mobile technology applications can bring viruses, malware and spyware into the organization’s network thereby creating a threat to the integrity of the institution’s data and IT infrastructure (Johnson, McGuire & Willey, 2009). Malware is defined as malicious software that intentionally harms normal computer software. Malware includes viruses, spyware, data miners, Trojan horses, and other programs designed to damage or destroy a computer (Malware, n.d.). Spyware is any software that covertly gathers information about a user while he/she navigates the Internet and transmits the information to an individual or company that uses it for marketing or other purposes; it may be installed along with other software or as the result of a virus infection (Spyware, n.d.).

While regularly updating antivirus and anti-spyware software and setting up strict security protocols, and enforcing network access controls can protect the information and files of the institution, it cannot really protect the academic institutions from targeted, persistent, and specific intrusions aimed at stealing, modifying or destroying information. A critical aspect of the process of mitigating the negative impacts of these risks lies in getting the people who access the institutions’ networks, whether through wired terminals or wirelessly via their laptops or mobile devices, to be aware of these risks and to practice safe computing.

This study looks at the online behavior of the respondents, specifically, sending and receiving attachments like videos, photos and documents that may allow the introduction of viruses into the recipients' mobile phones or laptops via email, and sending links to external websites that could be potential sources of malware while chatting and instant messaging. This study will also determine the respondents' level of awareness of the risks associated with the use of these mobile technologies and applications. Knowing how well their students understand the impact of risky online behavior will help this university's faculty and administrators address the gaps in policies and procedures that are employed by the institution to protect its I.T. infrastructure and its digital assets. While no generalizations can be made using the data gathered from this tiny sample, the conclusions and recommendations made at the end of this article will be of use to others in the academic community.

Background of the Study

The Philippines has an estimated population of 99.9 million as of 2010, 29.7 million of whom are Internet users (Internet World Stats, 2010). It has a mobile phone to landline ratio of nearly 17:1 (International Telecommunication Union (ITU), 2008b, 2010b). Considered the texting capital of the world, it has over 68 million mobile phone subscribers, with over 75 mobile phones per 100 inhabitants (ITU, 2008c, 2010a). In its Asia-Pacific Telecoms/ICT 2008 report, the ITU estimated that in 2007, each mobile subscriber in the Philippines sent over 400 text messages per month (ITU, 2008a). According to Wikipedia (2010), the largest average usage of the service by mobile phone subscribers is in the Philippines with an average of 27 texts sent per day by subscriber.

The focus group of this study are third and fourth year Business Management undergraduates enrolled in the extension program of a state university. Sixty-nine of the respondents were female, thirty-one were male. Of these respondents, forty-six were below 20 years old. Fifty-three of the respondents are third year students, the rest are in their senior year. This academic unit rolled out a wireless network in mid-2008; prior to this, a wired network was in place to serve both faculty and staff. Student access to the wired network was very limited. Only those enrolled in information technology-related classes held at the computer laboratory could access the Internet and the WWW via the wired network. However, the limitations on Internet and WWW access within the campus were eliminated when the wireless network came online in 2008.

The profile of the respondents shows that all of the students surveyed have cellphones (models ranging from the very old/hand-me-downs to the latest high-end web-enabled ones, brands ranging from the very inexpensive local or China-made phones to Nokias and iPhones). Over seventy of the respondents have had cellphones since they were in grade school and that all of the respondents have access to the internet.

All the respondents own or have access to laptops, netbooks or other Internet-ready mobile devices. These mobile devices are used to communicate with their peers, teachers and family members. The more sophisticated cellphones or smartphones allow the students to transmit and store documents via Bluetooth or MMS, take photos and videos, and share these friends and family. The respondents with access to pre-paid or post-paid wireless connectivity plans can use their cellphones to access the Internet and the World Wide Web (WWW) to surf, chat or browse. The increasing availability and affordability of wireless devices and services in the Philippines has played a major role in the growing use of mobile technologies among students. For the equivalent of just USD 10 or 450 in the local currency, a mobile subscriber can have unlimited phone calls and SMS, and twenty hours of internet access every month.

Marc Prensky's (2001) term for people who have been exposed to and have been familiar with information technology (I.T.) practically since birth – 'digital natives' – certainly applies to the respondents. They obviously have no difficulty using different types of mobile technologies and applications in their academic as well as their personal lives. The respondents use the wireless capabilities of their laptops and netbooks (802.11g, Firewire, and Bluetooth) to download, send and receive documents and multimedia files. Since the academic unit's wireless network is available for student use, they use the bandwidth to browse, do research for their course requirements, send and receive messages via email, chat or instant messaging (IM).

Methodology

I created a short survey featuring two types of questions. The questions belonging to the first type consist of a series of statements using a five-point Likert scale response pattern (Strongly Disagree, Disagree, Neutral, Agree, and Strongly Agree). The second type of questions asked the respondents to select from a given set of measures.

The total student population of the academic unit studied is 625, inclusive of graduate and undergraduate students. The survey forms were distributed on the last day of the semester, a day normally reserved for short wrap-up sessions. These forms were collected at the end of each of the four classes included in the survey. The sample size for this survey is limited to 105 undergraduate students enrolled in two information technology subjects. Five students enrolled in both subjects were asked to respond to the survey only once, resulting in a final sample size of 100 respondents. All responses were optional and respondents remained anonymous.

Findings

To evaluate the respondents' level of awareness of the risks associated with the use of mobile and wireless technology applications, particularly texting, email, chat, and instant messaging, three research questions needed to be answered: When the respondents use mobile technologies, with whom do they communicate and for what purpose? What kinds of information do the respondents send or receive? Are the respondents aware of the risks associated with the use of mobile technologies to access the Worldwide Web and the Internet?

When the Respondents Use Mobile Technologies, with Whom Do They Communicate and for What Purpose?

The survey presented five entities as possible recipients of mobile communications, namely: Teachers, Administrators/Staff, Family, Friends, and Other students. The respondents were asked to select from two types of messages, the School-related and the Non-school-related/Personal. The respondents selected which entities they communicated with and which types of messages they sent using the three mobile computing applications included in the study, chat/IM, email, and SMS. Table 1 summarizes the results gathered.

Table 1. Types of messages exchanged using mobile technologies and applications

Message Type	School-related only			Nonschool-related/ Personal only			Both			Neither		
Mobile App. used	**Chat /IM**	**Email**	**SMS**	**Chat /IM**	**Email**	**SMS**	**Chat /IM**	**Email**	**SMS**	**Chat /IM**	**Email**	**SMS**
Teachers	74	85	69	1	2	0	18	8	23	7	5	8
Admin./ Staff	37	44	46	3	2	2	13	10	12	47	44	40
Family	0	0	0	44	38	30	52	56	70	4	6	0
Friends	0	2	0	6	5	5	94	93	95	0	0	0
Other Students	19	20	12	3	2	0	73	72	83	5	6	5

Teachers received messages that were mainly school-related though several respondents indicated that they also sent nonschool-related messages to their teachers. The respondents preferred mode of communicating with faculty on school-related matters was email (85%), followed by chat/IM (74%) then by SMS (69%). Twenty-three of the respondents that sent both types of messages used SMS; eighteen used chat/IM. All told, ninety-two to ninety-five percent of the respondents communicated with their teachers using chat/IM, email or SMS.

An informal follow-up interview of the nineteen full-time faculty members at this academic unit revealed that all the faculty members allowed their students to communicate with them after class hours, particularly about curricular matters. However, only ninety-five percent accepted late evening or weekend communications from their students. Their preferred modes of communication with students were by texting and by email. Ninety percent accepted email from their students; all but three allowed their students to send them text messages. Forty-two percent of the faculty agreed to chat/IM with students but only on school days, never on weekends and seldom in the evenings. More than fifty percent of the faculty interviewed allowed their students to call them on their cellphones. Half of the teachers permitted students to discuss extra-curricular matters. Surprisingly, a little over a third of the faculty allowed students to discuss even personal problems and career plans.

Fewer respondents communicated with administrators or staff regarding school-related matters. Those who did used SMS (46%), followed by email (44%) then by chat/IM (37%). A small number sent both types of messages using chat/IM (13%), followed by SMS (12%) then by email (10%). Significantly, forty to forty-seven percent of the respondents indicated that they did not send any type of message to administrators or staff at all.

The respondents clearly used mobile communications to keep in touch with their families. The majority of the respondents sent both types of messages with seventy using SMS, fifty-six using email, and fifty-two of the respondents using chat/IM. Interestingly, some respondents communicated with their families on nonschool-related or personal matters only. Of these respondents, forty-four used chat/IM, thirty-eight used emails, and thirty used SMS.

Not surprisingly, the majority of respondents used mobile communications to send both school- and nonschool-related messages to their friends. Ninety-five of the respondents used SMS; ninety-four used chat/IM while ninety-three used email.

Fewer respondents sent both types of messages to other students. Of these, eighty-three used SMS, seventy-three used chat/IM, and seventy-two used email. Some respondents communicated with other students only on school-related matters with twenty using email, nineteen using chat/IM, and twelve using SMS.

What Kinds of Information Do the Respondents Send or Receive?

Given the number of respondents who communicate with their peers, teachers, family, and school administrators, an understanding of the kinds of information that they exchange with them is important. The respondents' online behavior – accessing links to websites, downloading files attached to emails, and downloading photos, images or multimedia files – can expose the recipient's mobile device (and the network to which the device is connected) to malware.

Certain procedural and access controls are in place to help protect the university's networks and information resources. Aside from automatic daily antivirus updates for all of the computers in the institution, students are instructed to have their personal USB storage devices checked for viruses and malware by a technical assistant before being plugged into any of the computers in the computer laboratory. This is done to minimize infection and re-infection of the networked PCs in the lab. Access to identified non-academic sites (examples are social networking sites, auction and ecommerce sites, sites with pornographic content, online gaming and gambling sites) is blocked, reducing the usage of the unit's computing resources for non-academic purposes.

Many of the respondents own smartphones – defined as a mobile telephone with computer features that may enable it to interact with computerized systems, send e-mails, and access the web (Smartphone, n.d.) – making it possible for them to send links, documents and multimedia files using text messaging or by Multimedia Messaging Service (MMS). MMS is a method of transmitting graphics, video or sound files and short text messages over wireless networks, especially on mobile phones (MMS, n.d.). However, MMS costs significantly more than an ordinary 160-character text message.

Table 2a shows that sixty-seven of the respondents use email to send links to websites, sixty use IM/chat, and roughly, a third of the respondents used text messages to send website links. Eighty-two of the respondents sent documents via email while sixty-six sent these during instant messaging or chat sessions. Only thirty-eight of the respondents (those with smartphones) used text or MMS to send documents. Eighty-five of the respondents used email to send photos or multimedia files while eighty used instant messaging/chat. Not surprisingly, because of the cost and the need for smartphones, only twenty used MMS.

Table 2a. Information sent by the respondents using mobile technologies and applications

Do the respondents send to people they communicate with messages which include:	Via instant message/chat			Via email			Via text message or MMS		
	Yes	No	Don't Know	Yes	No	Don't Know	Yes	No	Don't Know
A link or links to websites?	60	33	7	67	31	2	32	67	1
Documents, presentations or spreadsheets as attachments?	66	29	5	82	17	1	38	59	3
Photos, graphic images or multimedia files as attachments?	80	15	5	85	14	1	20	78	2

Table 2b shows that seventy-five of the respondents receive links to websites in email messages, sixty-eight via instant messaging/chat, and thirty via text messages. Eighty-five of the respondents had received documents as emailed attachments while seventy-one received these during IM or chat sessions. Only forty-one received documents via MMS. Eighty-eight of the respondents had received photos or multimedia files via email; a nearly equal number, eighty-seven, received these types of attachments during IM or chat sessions. A quarter of the respondents received these via MMS.

Table 2b. Information received by respondents using mobile technologies and applications

Do the respondents receive from people who communicate with them messages which include:	Via instant message/chat			Via email			Via text message or MMS		
	Yes	No	Don't Know	Yes	No	Don't Know	Yes	No	Don't Know
A link or links to websites	68	29	3	75	24	1	30	69	1
Documents, presentations or spreadsheets as attachments?	71	27	2	85	14	1	41	58	1
Photos, graphic images or multimedia files as attachments?	87	12	1	88	12	0	26	73	1

In summary, Table 2a showed that the respondents preferred to use email to send links to websites, documents and multimedia files; instant messaging or chat sessions come in as a close second. Text messaging or MMS was the least preferred method. Table 2b showed that the respondents were likely to receive documents and multimedia files through email or during IM/chat sessions. Text messaging and MMS provided an alternative though lesser-used route.

The data in Table 2a and 2b highlight an important fact: the sending and receiving of links to external websites as well as documents and multimedia files as attachments, using mobile applications like email, instant messaging, chat, or text messaging applications is common and happens frequently. This raises the likelihood that the University's information resources and confidential files can be exposed to viruses, spyware, and malware. While the University has firewalls and intrusion detection and prevention systems in place as well as procedural controls such as passwords and access control protocols to protect its networks and storage devices, the respondents' lack of awareness of the dangers of unsafe computing means that the University's systems, networks and storage devices are at risk from people who might want to attack the network, then steal, modify or destroy its information assets. But do the students realize this?

Are the Respondents Aware of the Risks Associated with the Use of Mobile Technologies to Access the WWW and the Internet?

Any place, any time connectivity is the main driver of mobile communications technology usage. The benefits are numerous but so are the risks associated with its use. Of immediate concern to academic institutions is the security of its networks and data in the face of increased access and usage by students for legitimate academic purposes. While inappropriate use of university network and computing facilities for mobile spamming, online gambling, and access to adult services pose equally important challenges to the university, the major issues considered in this survey are threats from viruses, spyware or malware, and threats to data security. The third research question attempts to ascertain the respondents' level of awareness of the risks the university's networks and data can be exposed to through unsecure mobile communications.

Table 3a shows forty-eight respondents agree that using chat/IM without adequate safeguards can expose the school network to viruses, spyware or malware; another thirty-one strongly agreed with the statement. Greater awareness that the use of email without safeguards posed a danger is revealed by the fifty-three that agreed and the twenty-four that strongly agreed. It is surprising to note, however, that only twenty-nine of the respondents agreed that unsecured cell phones could potentially expose the university's network to viruses, spyware or malware with only six strongly agreeing to the statement.

Table 3a. Level of agreement that using mobile communications without adequate safeguards can expose the institution's network to viruses, spyware or malware.

Awareness of the risks to the institution's network from viruses, spyware or malware	**SD**	**D**	**N**	**A**	**SA**	**NR**
Using Chat or IM applications without adequate safeguards can expose the school's network to viruses, spyware or malware.	1	5	15	48	31	0
Using email without adequate safeguards can expose the school's network to viruses, spyware or malware.	1	5	17	53	24	0
Using SMS or texting without adequate safeguards can expose the school's network to viruses, spyware or malware.	10	21	33	29	6	1

Key: SD = Strongly disagree D = Disagree SA = Strongly agree A = Agree N = Neutral NR = No Response

Table 3b mirrors the data in Table 3a, showing the same levels of awareness that using mobile communications without safeguards can endanger the University's confidential files and academic information. Also mirrored is respondents' lack of awareness of the potential risks that open, unsecured Bluetooth connections pose to the university's data and files.

Table 3b. Level of agreement that using mobile communications without adequate safeguards can compromise the security of the university's confidential files & data.

Awareness of the risks to the security of confidential files and financial data.	SD	D	N	A	SA	NR
Using Chat/IM without adequate safeguards can compromise the security of the University's confidential files & financial data.	1	6	17	48	28	0
Using email without adequate safeguards can compromise the security of the University's confidential files & financial data.	1	9	17	54	19	0
Using SMS or texting without adequate safeguards can compromise the security of the University's confidential files & financial data.	8	23	33	29	7	0

Key: SD = Strongly disagree D = Disagree SA = Strongly agree A = Agree N = Neutral NR = No Response

Discussion

The potential of mobile technologies and communications applications to support teaching and learning in this academic setting is clear. This study showed that the students were comfortable with mobile computing and that mobile technologies were easily accessible to them. Mobile technologies and communications applications allowed them to complete tasks and to coordinate activities, both curricular and extra-curricular, as well as to keep in touch with their teachers, both on a personal and a professional level.

The study also showed that respondents recognize that using mobile communications to keep family members informed about both school- and nonschool-related activities is a good way to foster a sense of community and involvement. It also allows students to appreciate the support structure that family, the university, and friends provide.

The online behavior exhibited by the respondents – sending and opening links to interesting or useful websites, and sending and downloading documents, photos and multimedia files – is characteristic of their age group and interests. While these students understood the benefits as well as some of the risks associated with the use of mobile communications applications like chat/IM and email, they still need to appreciate the threats posed by mobile phones, smartphones, the use of MMS, and Bluetooth connectivity better.

To further illustrate the seriousness of the threat posed by mobile malware to institutions, a brief overview of mobile malware, the vectors or methods that malware creators use to infiltrate networks and computer systems, and a few choice examples of the impact of malware intrusions on academic institutions are discussed below:

An Overview of the Threat from Mobile Malware

Recent threat bulletins from network security firms such as Juniper Networks and McAfee Labs offer a chilling picture of the alarming increase in malware threats to mobile and smartphone platforms such as the Symbian, Java 2 Micro Edition (J2ME), Android, and Windows Mobile between the years 2009 and 2010. The number of pieces of new mobile malware in 2010 increased by 46 percent compared with 2009. According to McAfee Labs, nearly 55,000 new malware threats are created every day. Of the almost 55 million total pieces of malware McAfee Labs has identified, 36 percent was created in 2010 alone (Bueno et al., 2011; Dignan, 2011; Juniper Networks, 2010).

Kaspersky Labs, another provider of IT security applications and services, has found that malware writers have started targeting the J2ME platform. All modern mobile phones, not just smartphones, as well as most laptops and netbooks support Java and can run Java applications that can be downloaded from the Internet, significantly increasing the potential targets for malware (Gostev & Maslennikov, 2009; Maslennikov, 2011).

Malware Target: Mobile Computing and Communication Devices

Mobile phones using the Symbian platform are key targets for smartphone viruses. This type of virus is a Trojan virus deposited in a phone with an open Bluetooth connection. It is used to steal information or send messages to pay-per-minute telephone numbers (smartphone virus, n.d.). A Trojan virus is a malicious, security-breaking program that is disguised as something benign, such as a directory lister, archiver, game or a program to find and destroy viruses (Trojan horse, n.d.). Nokia's Symbian remains the most targeted for malware – largely due to market share – but the increasing popularity and affordability of Android-based mobile devices have made the Android platform a prime target for malware exploits as well (Dignan, 2011; Rowan, 2011).

Bluetooth viruses, created in the Philippines as a proof-of-concept virus named Cabir in 2004, are programmed to signal any Bluetooth-enabled device (cellular phone or laptop) in the vicinity to accept a new application (Bluetooth virus, n.d.). Unsuspecting mobile device owners may allow the installation of these applications, thinking that a free video or game is being offered to them. Bluetooth viruses embedded in these applications may have a virus payload that can propagate and overload a network, destroy files indiscriminately, or deny legitimate users access to the network and the applications and files stored in an institution's hard disks. Since 2005, virus writers have developed hybrid malware that spread using Bluetooth and MMS connections (Runkle, 2009).

Malware Target: USB Mass-Storage Devices

Mobile computing and communication devices are not the only vectors for malware intrusions. The affordability and ubiquity of portable USB storage devices – usually a memory stick or thumb drive, but can also be any device with a mass-storage capacity such as a video game console, digital camera, cellular phones, and mp3 players – have made these devices a major target for malware.

Malware attacks and exploits in many universities have been traced back to infected USB storage devices that were plugged, unscanned, into computers connected the universities' networks. The infected device starts an executable file, which then invites a wide array of malware into the computer. The incoming malware copies itself into the core of the Windows OS and can replicate itself each time the computer is started ("Autorun for malware", 2010).

In late 2010, Western Illinois University experienced a widespread infection of over 700 university computers spread primarily via infected USB drives. The bulk of the infections (approximately 400 computers) involved public access computers such as those in laboratories and the university library (Rodriguez, 2011).

Whether spread via mobile phones, laptops, or USB devices, malware intrusions can wreak havoc on an institution's network, causing work disruption, the loss of institutional data and confidential files, identity theft and theft of personal information, and in some recent cases, the loss of significant amounts of money through fraudulent financial transactions. Below are just a few examples of the impact of malware intrusions in academic institutions:

Work Disruption

In 2009, Oxford Brookes University was hit by a significant and sustained Conficker worm attack on their network, causing work disruption spanning several days as shared student PCs and those used by its staff had to be scanned and cleared of the virus before these users could connect to the network again (Raywood, 2009b). The same worm also attacked the University of Utah where 700 campus computers and the computers that belong to the three hospitals on the school's campus were infected (Chowdhry, 2009).

Theft of Institutional Information, Intellectual Property and Confidential Files

The theft or destruction of data, intellectual property, proprietary research, and confidential files is of particular concern to universities. In one incident in 2009, University of East Anglia's Climatic Research Unit's email system was hacked. Information stolen from one of the university's servers used for research was made available on public websites and published without permission (Raywood, 2009c).

Pennsylvania State University (2009) reported network breaches caused by malware infections. These occurred at the Eberly College of Science (affecting 7,758 records), the College of Health and Human Development (affecting 6,827 records) and one of Penn State's campuses outside of University Park (affecting roughly 15,000 records).

Identity Theft and Theft of Personal Information and Communications

Impersonating a student of the University of London in 2006 allowed a hacker to access university computers, enabling him to infect the network with malware. The hacker used the "Cain and Able" program to hack student passwords and intercept network traffic. Using this program, the hacker was also able to access hundreds of emails containing the personal and financial details of students. Some of the stolen information was later used in fraud (Constantin, 2010).

Fraudulent and Unauthorized Financial Transactions

Malware like the Zeus Trojan steals personal information and business banking details that have caused millions of dollars in business losses in the US and UK in 2010 alone. Academic institutions have not been spared. The Marian University lost more than $186,000 in 2009 when thieves, using malware to penetrate the university's Finance Department computers, initiated bogus payroll transfers.

As a final example of how malware can facilitate fraudulent financial transactions, cybercriminals stole funds from University of Virginia in 2010 after compromising a computer belonging to the University's Financial Controller. Malware intercepted the online banking credentials for the University's Bank accounts and initiated a fraudulent wire transfer for $996,000 to a bank in China (Appleyard, 2010; Raywood, 2009a; Rowan, 2011).

In the face of the increasing frequency and sophistication of malware attacks, what can an academic institution do to prevent or at least mitigate the impact of attacks to its IT infrastructure and to protect its information resources?

Recommendations

While the University has firewalls and intrusion detection devices as well as procedural and network access controls in place, a critical aspect of the process of mitigating the negative impacts of these risks lies in getting the users who access the networks, whether through wired terminals or wirelessly via their laptops or mobile devices, to be aware of these risks.

Although it is impossible to eliminate all risks and vulnerabilities associated with the use of mobile and wireless technologies, a reasonable level of overall security can be realized by implementing a systematic approach to assessing and managing risk (Choi, Robles & Kim, 2008). This goes beyond simply investing in technology to protect the institution. User training, policies and procedures also play very important roles.

According to Turban et al. (2008), the major objectives of the defense strategies against network intrusions are prevention and deterrence, detection, limitation of damage, recovery, correction, and awareness and compliance. Using these defense objectives as guides, the following are some recommendations to protect the university's information resources and IT infrastructure:

Do not assume that users know the basics. Train users in safe computing practices.

The need to train and educate users in safe mobile and wireless networking procedures cannot be over-emphasized. It was suggested in Choi et al. (2008) that institutions and users would benefit from courses in safe computing practices and procedures. These courses should be scheduled at regular intervals, not just when the institution's networks and I.T. infrastructure are under attack.

Embed topics in safe computing and online risk awareness in introductory courses.

Academic institutions can include topics on safe computing practices in introductory courses or as part of orientation programs for incoming students. Stressing why students will benefit from being aware of the online threats and risks and from practicing safe computing can help them appreciate fully what needs to be done. Prevention is definitely better than cure.

Users tend to forget. Remind them often of the consequences of malware intrusions.

Guld & Guld (2009) recommend sending out regular reminders on the need to get the latest virus definitions for installed anti-virus software, installing and regularly updating anti-spyware and anti-adware applications, exercising caution when opening email from unknown senders or when downloading documents, photos or multimedia files.

Employ and enforce Acceptable Use Policies.

The University has an Acceptable Use Policy (AUP) and actively enforces the provisions of this policy for all types of users – students, staff, and faculty – of the university networks and computing facilities. But beyond simply ensuring students are aware that there is an AUP in force by displaying the AUP information screen and having the user acknowledge having read the terms and conditions of use, the administrators should take the time explain why there is such a policy in place in the first place. A clear understanding of why there is a need to protect the IT infrastructure of the institution as well as its information resources will go a long way towards getting users to observe the terms of use delineated by the AUP. Equally important is the need to discuss the penalties for violating these terms and conditions. It is vital for the all users of the University's network and computing resources to know that the University is serious about protecting its IT infrastructure and its information resources.

Keep your operating system updated with the latest security patches

Your operating system (OS) needs the updates, security patches and fixes that are available from the developer of the OS. These updates, patches and fixes are created and deployed in response to vulnerabilities exposed and exploited by malware writers. Failing to update or to apply the patches and fixes may mean that your system security has 'holes' that can be exploited.

Keep your antivirus and anti-spyware software updated

Make sure that your antivirus and anti-spyware applications are set-up to update automatically. The virus engine and virus definitions need to be updated constantly to keep your system safe from the latest malware and virus variants. Enable the on-access auto-scan feature of your antivirus software to force the scanning of files before use.

Use firewalls as your first line of defense but not your only defense

Firewalls serve as barriers between a secure network and the Internet, which is considered unsecure. Be aware that having a firewall does not stop viruses because these can pass through the firewall hidden in email attachments. Instant messaging and wireless traffic can slip through firewalls and effectively carry malware into the network. Finally, firewalls cannot control the actions of disgruntled employees or authorized users who unwittingly introduce malware into the network. Essentially, firewalls are a necessary but insufficient defense (Turban et al., 2008).

Keep USB malware off the network by restricting USB access

USB devices are a key attack point for malware. USB drives should be scanned before being plugged-in to a computer connected. Disable USB ports for users who do not need them.

Conclusion and Future Research Directions

One challenge for academic institutions is to be able to foster learning and creativity, to encourage cooperation and a sense of community, to cultivate a respect for intellectual property, and to advance the search for knowledge in a world made nearly borderless by mobile technologies. With the speed at which more sophisticated viruses and malware are being created and unleashed on organizations and institutions, another challenge for institutions face with tight budgets is putting in place, upgrading, and constantly updating the infrastructure, policies and procedures to protect its digital assets, yet still promote the ideals that an academic institution stands for.

An area of interest for future research is the role of academic libraries in promoting safe computing. Do libraries really provide the necessary guidance and support to encourage users, specially the youth, to practice safe computing? How can librarians achieve this in the face of shrinking budgets and the perception that academic libraries are becoming obsolete?

Finally, a study on the use or misuse of school computing networks and facilities for inappropriate or non-academic purposes is important in developing countries where budgets for equipment and services are miniscule while student populations are huge. Knowing how users utilize the available computing facilities and services will allow administrators to implement the appropriate controls to ensure that everyone – students, faculty and staff – gets to utilize the available computing resources to accomplish legitimate academic and administrative tasks.

References

Appleyard, K. (2010). University loses nearly 1 million dollars to malware. Retrieved from http://www.finextra.com/community/fullblog.aspx?id=4420

AutoRun for malware: One out of every eight attacks comes via a USB device. (2010). In *Avast.com*. Retrieved from http://www.avast.com/pr-autorun-for-malware-one-out-of-every-eight-attacks-come-via-a-usb-device

Bluetooth virus. (n.d.) *Computer Desktop Encyclopedia*. (1981-2008). Retrieved from http://encyclopedia2.thefreedictionary.com/Bluetoothvirus

Bueno, P., Dirro, T., Greve, P., Kashyap, R. , Marcus, D. , & Masiello, S. , ... Wosotowsky, A. (2011). McAfee Threats Report: Fourth Quarter 2010. *McAfee Labs*. Retrieved from http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2010.pdf

Castleman, W., Harper, R., Herbst, S., Kies, J., Lane, S. & Nagel, J. (2001). The impact of mobile technologies on everyday life. In *CHI '01 Extended Abstracts on Human Factors in Computing Systems* (Seattle, Washington, March 31-April 05, 2001). CHI '01. ACM, New York, NY, 227-228. DOI: 10.1145/634067.634202

Choi, M., Robles, R. & Kim, T. (2008). Wireless Network Security: Vulnerabilities, Threats and Countermeasures. Retrieved from http://whitepapers.techrepublic.com.com/abstract.aspx?docid=2251125

Chowdhry, A. (2009). Conficker Computer Worm Virus Attacks University of Utah. In *Pulse 2*. Retrieved from http://pulse2.com/2009/04/12/conficker-computer-worm-virus-attacks-university-of-utah/

Constantin, L. (2010). Hacker Impersonates Student to Install Malware on University Computers. In *Softpedia*. Retrieved from http://news.softpedia.com/news/Hacker-Impersonates-Student-to-Install-Malware-in-University-Campus-169002.shtml

Dignan, L. (2011). McAfee: Malware going mobile. In *ZDNET*. Retrieved from http://www.zdnet.com/blog/btl/mcafee-malware-going-mobile/44549

Gostev, A. & Maslennikov, D. (2009). Mobile Malware Evolution: An Overview, Part 3. In *Securelist*. Retrieved from http://www.securelist.com/en/analysis/204792080/Mobile_ Malware_Evolution_An_Overview_Part_3

Guld, J. & Guld, C. (2009). Practice Safe Computing. Retrieved from http://geeksontour.com/files/safe.pdf

International Telecommunication Union (2008a). Asia-Pacific Telecommunication/ICT Indicators. Retrieved from http://www.itu.int/ITU-D/ict/publications/asia/2008/APTI_08_Final.pdf

International Telecommunication Union (2008b). Basic indicators: Population, GDP, ratio of mobile cellular subscriptions to fixed telephone lines. Retrieved from http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/BasicIndicatorsPublic&RP_intYear=2008&RP_intLanguageID=1/WTI_BasicIndicatorsPublic.pdf

International Telecommunication Union (2008c). Mobile cellular, subscriptions per 100 people. Retrieved from http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/ CellularSubscribersPublic&RP_intYear=2008&RP_intLanguageID=1/WTI_CellularSubscriberPublic.pdf

International Telecommunication Union (2010a). The World in 2010: ICT Facts and Figures. Retrieved from http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf

International Telecommunication Union (2010b). Measuring the Information Society 2010. Retrieved from http://www.itu.int/ITU-D/ict/publications/idi/2010/Material/MIS_2010_without annex 4-e.pdf

InternetWorldStats.com (2010). Philippines Internet Usage Stats and Marketing Report. Retrieved from http://www.internetworldstats.com/asia/ph.htm

Johnson, M. E., McGuire, D., & Willey, N. D. (2009). Why file sharing networks are dangerous. *Communications of the ACM* 52, 2 (Feb. 2009), 134-138. DOI:10.1145/1461928.1461962

Juniper Networks Opens the First Global Threat and Research Center Focused Exclusively on Secure Mobility. (2010). In *Juniper Networks*. Retrieved from http://www.juniper.net/us/en/company/press-center/press-releases/2010/pr_2010_10_26-10_00.html

Malware. (n.d.). *Collins English Dictionary - Complete & Unabridged 10th Edition*. Retrieved from http://dictionary.reference.com/browse/malware

Pennsylvania State University (2009). Malware infections continue to be problematic for University. In *Penn State Live*. Retrieved from http://live.psu.edu/story/43612

Maslennikov, D. (2011). Mobile Malware Evolution: An Overview, Part 4. In *Securelist*. Retrieved from http://www.securelist.com/en/analysis/204792168/Mobile_Malware_ Evolution_An_Overview_Part_4

MMS. (n.d.). *Collins English Dictionary - Complete & Unabridged 10th Edition*. Retrieved from http://dictionary.reference.com/browse/MMS

Päykkänen, K., Räisänen, H., & Isomäki, H. (2006). Mobile studying and social usability on a wireless campus. In *Proceedings of the 8th Conference on Human-Computer interaction with Mobile Devices and Services* (Helsinki, Finland, Sept. 12-15, 2006). MobileHCI '06, vol. 159. ACM, New York, NY, 269-270. DOI:10.1145/1152215.1152281

Perry, M., O'Hara, K., Sellen, A., Brown, B., & Harper, R. (2001). Dealing with mobility: Understanding access anytime, anywhere. *ACM Transactions on Computer-Human Interactions.* 8, 4 (Dec. 2001), 323-347. DOI: 10.1145/504704.504707

Prensky, M. (2001). "Digital Natives, Digital Immigrants". In: On the Horizon, October 2001, 9 (5). Lincoln: NCB University Press.

Qinyin, C., Davies, N., Grout, V. & Cunningham, S. (2009). Key Issues That Apply to Wireless Local Area Networks (WLANs) Technology from a Study of the Chinese Campuses and UK Equivalent. Retrieved from http://whitepapers.techrepublic.com.com/abstract.aspx?docid=1218929

Raywood, D. (2009a). American schools hit by cybercriminals who set up fraudulent cash transfers. *SC Magazine*. Retrieved from http://www.scmagazineuk.com/american-schools-hit-by-cybercriminals-who-set-up-fraudulent-cash-transfers/article/148950/#

Raywood, D. (2009b). Oxford Brookes University network hit by Conficker. *SC Magazine*. Retrieved from http://www.scmagazineuk.com/oxford-brookes-university-network-hit-by-conficker/article/151476/#

Raywood, D. (2009c). New data loss reported as University is hacked with emails published online. *SC Magazine*. Retrieved from http://www.scmagazineuk.com/new-data-loss-reported-as-university-is-hacked-with-emails-published-online/article/158301/#

Raywood, D. (2010). University of Exeter hit by virus attack which causes network to be shut down. *SC Magazine*. Retrieved from http://www.scmagazineuk.com/university-of-exeter-hit-by-virus-attack-which-causes-network-to-be-shut-down/article/161929/#

Rodriguez, M. (2011). USB Malware Proliferating. In University Technology. Retrieved from http://www.wiu.edu/university_technology/USBMalwareProliferating.php

Rowan, L. (2011). Security zone: Mobile malware is already costing you money. In *Computer Weekly*. Retrieved from http://www.computerweekly.com/Articles/2011/03/29/245664/Security-zone-Mobile-malware-is-already-costing-you.htm

Runkle, M. (2009). New study describes risk of mobile phone virus attacks. In *Notre Dame News*. Retrieved from http://newsinfo.nd.edu/news/11824-new-study-describes-risk-of-mobile-phone-virus-attacks/

Smartphone. (n.d.). *Collins English Dictionary - Complete & Unabridged 10th Edition*. Retrieved from http://dictionary.reference.com/browse/smartphone

Spyware. (n.d.). *Dictionary.com's 21st Century Lexicon*. Retrieved from http://dictionary.reference.com/browse/spyware

Trojan horse. (n.d.). *The Free On-line Dictionary of Computing*. Retrieved from http://dictionary.reference.com/browse/trojan horse

Turban, E., Leidner, D., McLean, E., & Wetherbe, J. (2008). *Information Technology for Management: Transforming Organizations in the Digital Economy*. (6th Ed.). NJ: John Wiley & Sons.

Waycott, J. & Kukulska-Hulme, A. (2003). Students' experiences with PDAs for reading course materials. *Personal and Ubiquitous Computing.* 7, 1(May. 2003), 30-43.DOI:10.1007/s00779-002-0211-x

Wikipedia.com (2010). Text Messaging. Retrieved from http://en.wikipedia.org/wiki/Text_messaging

Xinhao, X., Wei, Z., & Min, L. (2008). ICT-Based Learning - More Freedom, More Side-Effects? In *Proceedings of the 2nd international Conference on Next Generation Mobile.*
DOI:10.1109NGMAST.2008.46

Author Information

Maria Sagrario R. Simbulan is an Assistant Professor at the University of the Philippines Diliman Extension Program in Pampanga. She teaches information technology and technology management courses at the graduate and undergraduate levels. Her research interests include the use of IT in society, user interface design, learning objects, database design, and the use of technology in teaching and learning. Email: msrsimbulan@up.edu.ph