# Information Security Updates

## Mobile Computing

Issue 3

### Related Article

**Is Apple's iPad the Future of Mobile Computing in Education?**

Ball State University's professor predicted that the iPad will become a strong education device because of its interactivity and its ability to use converged media. The university currently has several mobile device programs running. About four years ago the campus introduced iPods in the classroom. They have found use in music, language, and biology classes, among others.

(http://campustechnology.com/articles/2010/01/27/apples-ipad-the-future-of-mobile-computing-in-education.aspx)

### Statistical Report

**Security at the Edge – Protecting Mobile Computing Devices**

There is compelling evidence that mobile devices pose one of the fast growing areas of security concern. Privacy Rights International's published Chronology of Data Breaches documents that ninety-one (91) of the 444 data breaches reported (20%) resulted from mobile device losses – lost laptops, notebook computers, PDAs, portable drives, USB drives, CDs, flash cards, SD cards, and diskettes.

(http://www.nascio.org/publications/documents/NASCIO-SecurityAtTheEdge.pdf)

# I. Background

The users' aspirations for easy access to information resources has spurred the demands for the use of mobile computing devices, e.g. PDA, laptop and Smartphone) through wireless network.

**Industry Story**

**The Mobility Effect**

By 2013, Internet Data Centre (IDC) predicts the number of Internet-capable mobile devices that will go online to reach 1 billion. Mobile phones will overtake PCs as the most common internet access device worldwide. More and more organisations in different industries have deployed mobile devices for higher efficiency in communication and collaboration, ushering in a new era of computing and employee productivity.

The strong growth of mobile computing also poses new concerns for data security. According to Symantec's Internet Security Threat Report, 63% of vulnerabilities reported in 2008 affected Web applications. In 2009, the first Smartphone botnet took advantage of users' contact lists to spread itself via SMS. See the article:
(http://www.computerworld.com.au/article/348611/mobility_effect/)

**Mobile Computing in Education**

The use of mobile computing within universities is expanding at an ever-increasing rate. While staff and students can enjoy the beauty of mobile computing, drawbacks also exist at the same time.

**Benefits**

1. **Mobility –** With access to educational information at any time and from any location with wireless coverage, teachers and students would benefit from great flexibility in communication, which improves the efficiency of faculty teaching, student learning and collaboration.
2. **Higher efficiency –** Today's portable computing devices provide a variety of functionalities such as organiser, instant messaging and video streaming, which allow better organisation of teaching / learning schedule, effective individual (one-to-one) mentoring process and enhanced teaching approaches.

**Drawbacks**

1. **Security threats** – Wireless signals are broadcasted in public area and can be easily captured by outsiders. Thefts of mobile devices not only cause economic loss but also result in potential leakage of personal information. Examples of the malware or spyware are FlexiSpy, QQsend and InfoJack.
2. **Higher security cost –** The inclusion of mobile computing devices adds complexity to the existing security management process. New security devices for mobile computing are needed and the IT management needs to conduct more awareness training for IT staff and users.

References:
http://clifmims.com/site/documents/MobileWireless-HigherEd.pdf
http://www.nascio.org/publications/documents/NASCIO-SecurityAtTheEdge.pdf

# II. Management

## Transition to Mobile Computing

Universities' management are responsible for evaluating the feasibilities and establishing an effective strategy when adopting mobile computing. An assessment on the key elements, including people, policies and technology, should be performed to determine the necessity and approach of mobile computing implementation in university environment.

### 1. People

A university's transition to mobile computing relies on an effective integration of wireless technologies into a higher education environment with proper commitment from management.

To support and manage its educators and students in a mobile environment, management should perform a comprehensive analysis of the user profiles. The major elements that should be assessed by management include:

- **Educational needs** – the criticality, time sensitivity, and user expectations of education and research activities that will be shifted to a mobile environment. Do they require a real-time response? What is the value added of moving to a mobile environment?
- **Access mode** – management should find out the approaches and locations that users gain access to university's information systems and resources. What kind of mobile devices do they prefer? How many different locations are involved, and are those locations used repeatedly or occasionally?
- **Usage patterns** – management should consider how educators and students utilise mobile technologies to perform their tasks. The variety of tasks includes presentation, tutorial, peer mentoring, self-learning, documentation, research study and program scheduling.

### 2. Policies

As mobile devices and information services are increasingly used in combination, universities need a comprehensive set of policies to ensure consistency of information security management, compliance of relevant laws and regulations, and an optimized achievement of educational objectives for mobile initiatives.

Policies should address the following key questions:

- Who is an eligible mobile user?
- What are the user responsibilities?
- What technology is provided and supported?
- What level of access and services are provided and supported?
- Who buys or owns the mobile devices?
- Who pays for the support and maintenance?

Developing comprehensive mobile policies cannot be done in isolation. It is crucial to involve all university key stakeholders, including management, educational staff, IT security personnel and students.

**Statistical Report**

**Mobile computing will outpace desktop technology in 10 years**

Mobile computing will outpace desktop technology in the next 10 years. There are challenges to access, security and interoperability issues to overcome, according to a study from the Pew Research Centre's Internet and American Life Project released on Friday.
The report, a survey of nearly 900 Internet and technology experts, found that 72 percent of respondents believed technology users will conduct business using shared mobile platforms and smart phone applications rather than desktop computing. Easy access to information and the growing use of mobile devices will be key drivers of this trend, they said.

(http://www.nextgov.com/nextgov/ng_20100611_7150.php)

**Related Article**

**U.K. officials ask Google to delete Wi-Fi data**

The U.K. government ordered Google to destroy personal data collected through the Street View project.
Google disclosed that it had inadvertently collected personal data from Wi-Fi hot spots as part of its Street View mapping project.
Privacy advocates in the U.K. were disappointed as Google initially told the German government and the public that it didn't collect this type of personal data before backtracking on that claim following an internal review of its software.

(http://news.cnet.com/8301-30684_3-20005289-265.html)

References:
http://www.computer.org/portal/web/csdl/doi/10.1109/MITP.2010.96

# II. Management (cont'd)

## 3. Technology

After management has analysed the mobile user profiles and defined the policies, there are technical decisions to be made:

- Selecting devices for each mobile user type;
- Setting the communication requirements;
- Defining security requirements and support technologies; and
- Formulating the support plan.

The following principles should be observed when making technical decisions:

1. Mobile solutions must align with the university's long-term mobility strategy. They should support the overall educational objectives and also allow for easy migration to new mobile platforms and support multiple platforms.

2. University must keep its sensitive information out of the wrong hands by carefully choosing mobile technology with built-in security features. For example, the devices should have encrypted hard drive, device tracking and recovery abilities, and user-authentication solutions such as integrated smart cards or biometric readers.

3. University should adopt reliable and centralised device management mechanisms to handle increased risks of device theft, data leakage and other security breaches resulted from mobile solutions. A competent mechanism, such as Blackberry Provisiong System and Microsoft System Centre Mobile Device Management, shall allow its IT administrators remotely shut down, diagnose, repair, and update a mobile device's system via secured channels.

4. University shall revise its existing security policies in response to the new security threats that come with the mobile computing technology. The revised security policies should cover the issuance of mobile devices, secure configuration, secured access control, travel considerations and device destruction. Corresponding security awareness training program shall also be delivered to mobile users before releasing the devices.

5. Regular risk assessment must be conducted by the university to identify any security vulnerabilities in its mobile network. The assessment may include a penetration test of wireless setup, a review of encryption measures being used for wireless communication and a revision of policies and procedures pertaining around wireless networking.

6. University should provide its IT administrators and support personnel with adequate technical training in relation to security hardening, device maintenance, and security incident management of mobile devices and infrastructure.

**Standard Update**

### Wi-Fi security in transition

802.11 Wi-Fi has gone through several security transitions in its basic encryption/authentication mechanism. Most enterprises upgrade to the latest versions as they buy the newest products, which support the highest form of 802.11 security, 802.11i, also called Wireless Protected Access (WPA) 2 and uses a form of AES encryption) The Wi-Fi Alliance deems WEP and WPA to be inherently insecure, it is now instituting a phased plan to prohibit the older protocols from its product certification testing.

(http://www.networkworld.com/newsletters/wireless/2010/070510wireless2.html)

**Related Article**

### Education technology executives meet to discuss key trends in school computing

Hosted by the Software and Information Industry Association (SIIA), a recent education technology industry summit was intended to keep company executives abreast of the latest trends and recent developments in school technology. But its content also gives educators a glimpse into where business leaders see the education through technology (ed-tech) industry heading.
Mobile technologies can provide 24-7 connectivity for learning. Mobile devices offer an emerging platform for the "21st-century textbook"—one that is more flexible, interactive, and allows for instant feedback, as well as greater personalization of the learning process.

(http://www.eschoolnews.com/2010/06/21/summit-mobile-computing-is-educations-future/)

References:
http://www.computer.org/portal/web/csdl/doi/10.1109/MITP.2010.96
http://www.informationshield.com/press04-17-2009.html

## III. General Users

Upon the deployment of mobile computing environment in the university, one of the issues contributing to a lack of security is the perception of general users that university mobile computing devices are also personal devices and there is little risk involved in common practices.

### Roles and Responsibilities

As the university mobile devices have real access to university data, general users should not use them for personal purpose and should comply with the university security policies. General users have an important role to ensure the security of their mobile devices and the university protected information.

### Good Practices

1. **Enable password protected screen / keyboard lock**
   Always enable this first line of defence in helping to protect the information in your mobile devices. It should be set to automatically lock the devices after being left idle for a predetermined amount of time (e.g. 5 minutes).

2. **Minimize storage of data on mobile devices**
   Try to store only minimum amount of data necessary on a mobile computing device for the shortest possible time required. For data that requires longer period of storage, move it to a more secure device and remove it from mobile device as soon as possible.
   Avoid storing confidential data in the mobile computing device. University protected servers should be the first option for storing confidential information.

3. **Encrypt your files**
   Make use of data encryption software such as WinZip as well as TrueCrypt for file encryption on university laptop. A strong key, created in line with the security policy, should be used for encryption when files are being transferred into removable media or through email.

4. **Do not use unauthorised wireless connections**
   Avoid connection to unauthorised wireless network, either unknown wireless networks or unsecured connection in a public place.

5. **Do not open messages from unknown sources**
   SMS or Multimedia SMS (MMS) from unknown or suspicious sources may contain malicious content and should not be opened when checking messages on mobile computing devices. Bluetooth function should be deactivated by default. Data transmission requests from unknown Bluetooth devices must not be accepted.

6. **Comply with security policies**
   Understand and follow the guidelines and best practices stipulated in the security policies. Consult IT security for any inquiries or arising information security related matters.

**Related Article**

**Mobile security needs more than just software, it needs education**

Lookout Mobile Security has seen a rise in the number of apps that are loaded with malware. Six months ago, four pieces of malware would be found per 100 phones per year. Today, that's jumped to 9 pieces of malware. And it's not just on open source platforms like Google's Android. There have been instances of problems with apps that get past the app judges on Apple's iOS platform, as well.

(http://www.zdnet.com/blog/btl/mobile-security-needs-more-than-just-software-needs-education/36437)

**Related Article**

**Increased mobility, increased risk**

Increasing mobility also means increased risk to security of computing systems, data and the welfare of the very businesses that use mobile devices. We know, for example, that growing use of social networking and video-sharing websites increases network exposure to viruses and malware. And contacting those sites via roving laptops or handheld devices, which tend to be harder to secure, only exacerbates the risk.

(http://www.computerworld.com/s/article/9178742/Increased_mobility_increased_risk)

References:
JUCC Information Security Updates – Data Leakage Prevention
http://searchmobilecomputing.techtarget.com/news/1269948/Mobile-security-is-end-user-and-IT-responsibility