Mobile Strategy for Binghamton University

Binghamton University Mobile Strategy

1.1 Introduction

“Mobile phones will overtake PCs as the most common Web access devices worldwide by 2013.” –Gartner Group (one of the world's leading information technology research and advisory company.)

The world is shifting to a mobile-dominated post-PC era in information technology (IT). The research firm Gartner predicted mobile phones will overtake PCs as the most common web access devices worldwide by 2013.[1] This shift is enabled by the convergence of three trends: the growing number of Internet-capable mobile devices,

1.4 Strategy Stakeholders and Review

- Student Affairs
- Academic Affairs
- Information Technology Services
- Communications and Marketing
-

We have also seen a continuous increase in Internet, with demand increasing at a rate of nearly 40% per year. To address this ITS has upgraded Internet capacity to keep pace with this trend.

To address the overall increase in Wi-Fi and Internet usage the backbone of the Campus network was upgraded in the summer of 2013, and the network infrastructure continues to be upgraded in a comprehensive manner.

1.7 Security

Binghamton University boasts a secure, robust Wi-Fi network in every building on campus. The residential living quarters are all Wi-Fi capable as well as all academic and administrative buildings.

The campus Wi-Fi network infrastructure is encrypted and has the ability to logically place students and faculty/staff on separate networks. This enables a security layer for administrative resources such as servers and shared drives that faculty and staff can access and that students cannot.

Binghamton University also provides an open wireless guest network named "Connect2BU." This wireless network was designed for use by prospective students and their families to connect to both the Internet and to campus informational resources, thereby enhancing their visit to the campus. It also serves as an on-boarding network for students, faculty and staff to provide easy to use instructions for connecting to the secure encrypted campus network.

Any data that we currently categorize as sensitive should be considered at risk with mobile usage. There is no reason to create new categories of data based on how someone accesses them. Mobile devices (to include laptops) are simply small computers. The security risks with mobile devices are compounded partially due to the ease of loss/theft of the device and the open approach of some mobile operating systems. Technically, a USB memory stick could be called a mobile device for the purposes of data security discussions as someone can carry it in their pocket, use it to store sensitive data and carry it off campus just like with a phone, tablet or laptop.

Mobile devices are the number one targets of thieves today. This can come from devices that are physically stolen or their control stolen by infected or misleading apps.

A device that is physically stolen can have sensitive documents on it, access to critical apps such as e-mail, company applications, social media accounts, etc. Faculty members may have important research their device. Staff members may have downloaded sensitive documents as e-mail attachments or other services. Students may have financial documents or access to various social media on their device. Any of these on a lost device could fall into the wrong hands.

Like desktop computers, mobile devices can be attacked by malware or just misleading apps. Misleading apps can look safe enough but may actually be stealing data, or may leave you holding the bill for surprising charges.

all of which can give rise to significant privacy and security concerns. Many times these can be disguised as anti-virus apps.

Another area of concern is “Data leakage.” Many mobile users sync data to their various mobile devices through free services like Drop Box. These services can get exploited and allow the files to be corrupted or stolen.

There is an inherent difficulty in securing mobile devices in the new “Bring Your Own Device” (BYOD) environment. Standards can and should be set for University-issued devices but securing a personal device remains with the diligence of the owner.

A comprehensive website on safe mobile computing needs to be created. Some of the suggested standards for personal devices and should be mandatory for University supplied phones:

1. Locking – this is a capability supplied on all smart phones that makes someone enter a password or swipe the correct pattern on the touch screen. New phones offer biometric access measures.
2. Remote wipe capability – offered through iOS for iPhones. For other phones there are services that provide this capability. This allows someone with a lost phone to wipe out everything, i.e. files, apps, photos, etc. from a remote location. With a good backup in place the wiped items can be restored on the phone if found or on a replacement phone.
3. Malware protection app – the same carriers of malware that plague desktops also are a threat to mobile devices—infected websites, file-sharing services, e-mail attachments. Old versions of Android also leave security holes.
4. Shop reputably – there are plenty of app stores claiming to have ‘the world’s widest selection,’ but independent app shops tend to be less regulated than those run by well-recognized tech titans like Google and Apple. Only authorize the downloading of apps from reputable vendors to circumvent the distribution of mobile malware into your organization.

A possible next level of protection would be encryption. This is a more dramatic measure where data on the phone is encrypted and cannot be accessed without typing in a password on power up. A risk assessment of possible loss should be undertaken to evaluate the need for this kind of protection.

Mobile devices such as smart phones and tablets can be set up to access most of the critical University communication services. Below is a list of the most popular:

- Any Wi-Fi enabled device will be able to connect to the BU wireless network. The website https://wireless.binghamton.edu has instructions to enable your device to access the network.
- Your mobile device can have its e-mail app setup to access the Universities B-Mail and calendaring.
- File sharing can be done through Google Drive on your b-mail account.
- In the near future there will be web-based access Qq services like

It should be noted that if faculty/staff wish to share data with non-affiliated individuals they will not be able to use something like our enterprise file sharing system.

1.8 Other Risks

1.12 Backend Systems

Backend systems that are in use by the University include:

- The University runs Ellucian’s student ERP product, *Banner*. Banner is accessed by both students and staff to process various academic functions such as course registration, billing, admissions processing, financial aid to name a few. Banner provides a non-mobile web presence. Authentication is done through Active Directory and the web pages can be reached outside of the firewall. The University is looking at options to make the Banner’s web presence responsive. A possible alternative for the pages that don’t adapt well to the responsive code is to develop Banner web services to be consumed by our existing mobile app, bMobi. Security of SIS data is of paramount importance as this development advances.
- Binghamton uses Blackboard’s learning management system for both faculty and staff. This also uses active directory and can be used outside of the University firewall. Blackboard provides a mobile application for its product that Binghamton has purchased and which is accessible from the University’s app, bMobi.
- The University runs Ex Libris *Aleph* product to handle it’s library processing. There is currently a mobile application being written to support this product.
- The University runs several different smaller systems that support specific functions on campus. At this point most of these systems don’t have a mobile component. However, the systems that deliver heavily used services should be prioritized for mobile development.

1.13 Mobile Service Delivery

Our current Mobile Service delivery is in a hybrid mode. We have responsive website pages and a native app. Currently having a responsive website that adjusts to any device is the best way to ensure a usable and effective mobile presence.

1.13.1 Off-the-shelf apps

Companies like Ellucian and Blackboard offer off-the-shelf mobile apps

1.13.4 Skills Development

Communications and Marketing staff have successfully led creative design, user experience (UX), information architecture (IA), implementation, testing and training in critical mobile areas to-date. ITS partnership has been critical to these successes. Continued success should build on existing skill set strengths in an increasingly cooperative manner.

1.13.5 Mobility Roadmap

- Responsive web first for all UAJs q 13.51oi5 11 71esp

- Tj ET Q q 0.06 0 0 0.064240.345 38 5439 cm BT 200 0 0 200 0 0 Tm /TT1 1Tf ex.:•