

ITEE Meeting: November 12, 2010

Assimilating Mobile and Consumer Devices into the IT Infrastructure

Fire alarms and exciting tours created an interesting kick-off to this ITEE meeting as eager participants soaked up the tours with great interest and then scrambled for the exits as the fire alarm reverberated throughout the Polsky Building and Taylor Institute.

Participants of this ITEE session were treated to a tour of both the Taylor Institute and the Suarez Neuro Marketing Lab conducted by The Taylor Institute's enthusiastic professor, Dr. Hauser. Numerous projects are underway at the Taylor Institute and many corporate donors provide the financing regarding several of the institutes' rooms and divisions of this fascinating department. Taylor contains a diversified mix of TV rooms, focus group rooms and computer labs providing real life working experiences for participating students. All funding derives from the private sector and firms have use of the facilities with the explicit agreement that all students have the opportunity to work alongside the actual employees of the donating firm on live projects.

George Mehok, our moderator, from Revol Wireless kicked off our exchange session with a historical overview of the cellular industry. He also showed us samples of popular cellular telephones spanning the last 20 years, creating a nostalgic atmosphere. A few moments after George began his presentation, the group was disrupted by a fire drill and that event cut our exchange time down by about 20 minutes. After the group reassembled, our undeterred moderator continued with his presentation as if nothing had happened and the group quickly refocused on the topic at hand.

George focused the discussion in two areas. The first area is supporting the devices for internal customers or end users. The second area is supporting external customers through use of applications. This is the customer facing aspect. The biggest challenge today is the "consumerization" of wireless devices within IT. (George created an interesting new word) It is difficult to prevent devices from accessing the network. Every time a new device hits the market, the device comes into the workplace. George is

most interested in the external aspects due to Revol's business model.

George then goes through an intriguing example of purchasing his iPad directly from his iPhone. After checking his e-mail and viewing a note from Giant Eagle indicating his current fuel perks, George notices a mall link on the Giant Eagle website where customers can purchase things and earn fuel perks. Apple was a link in this virtual mall so George decides to click it. Because George is interested in selling Revol services in this manner, he goes forward to find out how the Apple link really works. After logging in with his fuel perks login, he is directed to the Apple site indicating connectivity between the two sites. Apple immediately recognized that George was using an iPhone and it asked him if he wanted to download the Apple App necessary to purchase products at the Apple store. George downloads the app, clicks on the Apple store, and sees a full line of Apple products. Since George has been interested in purchasing an iPad, he decides to click on the link. After reviewing the device, George clicks the buy option and the system directs him to sign into his iTunes account. The iPad purchase charged directly to his iTunes account and immediately following, George receives an e-mail indicating that the order transmitted to China and a confirmation of the order was received. Twenty-four hours later, an e-mail generated to indicate where the iPad was in the shipping route and within 48 hours, George had the iPad in his hands. This is a great example of what is possible when a firm's e-commerce system, wireless, and affiliate partners are all integrated. The system makes it easy to spend money! Associates of your company will do this type of transaction and wonder why this cannot be done at our company. George is now tasked with how to do this for Revol.

Another situation sprang up where George's CEO had a DropBox application, used for storing documents in a cloud for retrieval from any location, and desired to begin using this service right away. The CEO then sends proprietary data into the cloud that causes security concerns. George elected not to explain this risk to the CEO.

Question: Why did you elect not to tell the CEO of the danger? George explains that Revol is a small private company and the information is not as proprietary as most. The next problem is that once George explains this problem, the CEO will ask him for the solution and this is the bigger issue. Encryption could be a solution and this is an expensive service. Data must be classified and policies must control data sharing. There is a constant battle with the “why can’t I” do this or that employees. In many cases, users need a client and a certificate to access the network. Physical control is an option used by many firms. In most cases, executives are the most demanding when it comes to accessing the system.

Support is another problem. Some industries adhere to strict guidelines concerning the security of credit card data. In George’s situation, the CEO desiring a WIFI network at the office opens the firm to even more guidelines and regulations that add costs. Compliance costs increase in order to allow users to access the system. It is important to document the costs related to supporting new devices. The company will provide guidance to the employee but indicates that the employee may need to contact their provider. In the case of an executive, you may have to do this yourself.

The best idea involves providing employees with a stipend for approved devices that can be used on the network. Then you can provide support and back-up devices. Firms cannot fight employees regarding end use devices because employee productivity increases with the devices usage. All of the information a company has must be available in a “gated community.” This is critical in a consumer facing business because the consumer uses these devices and it makes sense for the employee to be lead users.

Question: Does it make sense to invest in WIFI if you have a cellular network? Everything is converging into one as telecommunications evolve. There will be more cell towers as we go forward. Broadband demand is exploding. Trends indicate

that pay as you go models will be in effect. The cellular firm will charge depending on the service.

Question: Will people be aware of the variable pricing. Monthly bills will give way to micro transactions. This is how I-Tunes work. Sticker shock legislation will come forward. Credit cards will be linked directly to the device and will be charged in real time.

Question: Many firms desire to create applications that provide consumer visibility as the consumer walks into the store. What are the current retail trends in the cellular industry? Abercrombie and Fitch is developing an app that will locate the customer and send them special announcements as the customer comes close to a retail location. This will link through Face Book and Twitter. The app will contain intelligence that will hold the customers past purchases and make recommendation. The stores sales rep will also be notified and will be able to interact with the customer. This creates tremendous business intelligence. The hit rate will be much high with this style of direct marketing as compared with direct mail.

Question: Is there a way to lock down an iPhone? BlackBerry is the only phone that uses the Mobile Iron security system. There is software available called Travel that will allow control. Users would rather allow the company to control the device than losing the device altogether.

We need to build a culture of security because end users will be responsible for making the right choices. Will people make the right choices concerning the privacy of data? Not likely unless the user has been burned before. IT security training should be mandatory. Some firms can lock down the users system until the training is completed. Another issue is that employees will become personally liable for data breeches. The university is moving this direction. IT must be on top of the security issues that will continue to develop.

This Summary was prepared by Paul Evans, University of Akron