Global Information Assurance Certification Paper

Warren Bowyer
GSEC Practical Assignment V1.3

Mobile Computing, convenience at what cost ?

In this paper I will attempt to cover some of the prominent basics security concerns associated with the myriad of mobile technology devices being employed in the everyday business environment we work in.

I will also cover some of the possible tools and techniques available to try to keep control of these new security threats and suggest a possible user policy to apply to mobile device use.

Introduction

There was a time not so long ago when the IT department was either covertly or overtly, depending on the type of organisation, the driving force behind many changes in corporate and general office culture through the extended use of technology.

Whether you want to admit to it or not those in IT sometimes had to create our own demand for computer solutions in the companies we worked just to get our hands on the latest hardware and software. Although it was done with the best intentions we genuinely felt sure the increased use of technology would benefit all, but would also give us something more interesting to do and keep our skills saleable (if you have ever been in a company supporting the same legacy system for more than 3 years you will know what I mean).

Comparatively high cost and a general lack of knowledge and understanding of computing by business owners and managers initially kept them cautiously dipping their toes into the unknown depths of the computer sea and in many cases it was the IT department tha t had to be the one to drag them kicking and screaming into the water to prove they would not drown.

The realisation that computing was not so complicated and from a relative cost point of view is now accessible to all has both increased demand by companies to deploy technology whenever and where ever possible but also through increased understanding and awareness is generating at an ever increasing pace demand for more convenient customized solutions that run on open platforms and are portable to a whole host of mobiles devises.

Expectation and deployment of mobile and wireless computing devices is growing at such an exceptional/alarming rate it is now the IT departments that are struggling to keep up with the pace of change and is putting

evermore increased strain on what were probably already limited IT support resources.

It used to be that new software and technology was viewed with great suspicion by the IT informed for fear of bugs or support problems for months, even a year before anybody would risk to use it, which gave time to understand the issues and read the reviews and advisories before you were faced with them "live". Now the demand for ever newer and more convenient computing is having its toll on the IT department, making it difficult sometimes to keep pace with the daily changes in business demand and innovation and being able to keep control of issues such as security.

The history lesson and complaining aside, there are some very real consequences of the present speed of change in the mobile computing field and trying to meet business expectation, which is that, security being at the very opposite end of the convenience scale is very often an after thought in both emerging software and hardware design and what security considerations there are "out of the box" normally just about meet only those most basic expectation because the product generally is going to be sold based heavily on the strengths of its convenience and functionality, there is nothing exciting a salesperson can say about security.

IT support staff are also frequently not properly trained in set-up and support for some of these latest technologies and learn their way only as they go. There often is never enough research and development time because of the speed of demand and lack of training or money available to do anything more than just purchase the device and get it up and running.

Common Concerns

The most popular mobile device is the cell phone, this has long since become a standard business tool but initially was not considered such a security risk as it was used for primarily voice communication only. Today's cell phones are no longer so straight forward incorporate more functions than even the personal organizers of old including; contact data, scheduling, web access and email applications. Some of the major issues with mobile phones are that both voice and data is transmitted normally without any encryption and can easily, with the correct equipment be capture out of the air exposing any confidential information. The protocol and technology used for this type of communication was not designed with any real strong security in mind and even though many case have been reported of people having their numbers copied allowing criminal elements to make calls on the victims bill there currently is no comprehensive solution being provided by either the industry or

manufacturers, more security often means less convenience. Digital phones are considered a better solution because of standard encryption but the relatively higher cost and limited supply of supporting infrastructure and equipment has not made this a popular solution. As phones get smaller and cheaper, loss and damage becomes a more frequent occurrence, now that phones have increased memory capacities and the ability to host an operating system, scheduling, address, email and web access applications the risk that important or sensitive information gets lost or corrupted has greatly increased and will continue to do so as the data storage capacity and application functionality rapidly grows along with the development of the technology. As technologies merge and phones become PDA's and visa versa this problem will become compounded, RIM's BlackBerry wireless e-mail pager is an example of a device growing in popularity and bridging technologies.

"Wireless communication is now a staple of mobile business professionals everywhere who enjoy the convenience and increased capabilities that these devices offer. But while new features and capabilities abound, many experts agree that the security of information stored and transmitted by wireless devices remains a serious concern for wireless product vendors and their end-user customers"

[1] Major Obstacles Remain To Securing Wireless Devices, January 17, 2002, Leo Pluswick
http://www.trusecure.com/html/news/press/2002/prsecuringwireless011702.shtml

Next is the laptop computer, this has a host of security concerns spanning availability, confidentiality and integrity; the number one cause of non availability is physical deliberate or accidental damage rendering the machine inoperable, loss or theft comes in second.

"According to the most recent published study by Safeware (a PC insurance company) 309,000 Laptops were stolen in 1997, up 17% from the year before."

[2] February 7, 2002, What's the best Way to ensure your Notebook and (probably more important) your DATA doesn't get stolen?
http://www.notebookreview.com/security.html

Maintaining system integrity is also a big problem that comes in many forms; it can be very challenging for IT administrators to keep laptops up to date with the latest application and OS service packs and patches, already this is an enormous task for networked machines particularly if there is no standards within the company for OS and application platforms. There are now tools available to help monitor and automate the application of patches but there is still exposure especially from those

frequent travellers who rarely connect to the network or only connect over slow dial up lines.

Frequent travellers are also prone to not updating their own anti -virus profiles, this task again can now be automated for the machines attached to the network but this is not so straight forward for staff who's main contact with the main office is through a dial -up connection. Updates can be activated through an internet connection direct to the anti virus providers web site but again we are normally dealing with a slow dial up line.

Today's laptops normally come with built in modems which provide unprotected access to the internet, this has the effect of bypassing any security controls that may have been put i n place like the corporate firewall to protect against the threats inherent with the internet.

As for confidentiality, most business users do not have any encryption software available on their laptops which greatly increases the impact of theft as any da ta on the machine is easily retrievable and password controls are no match for anybody with readily available password cracking tools.

Unfortunately, even if the face of constant reminders many users still are not disciplined when it comes to making regul ar data backups and this frequently leads to an inability to recover from any machine failure or loss. Month old backups or older are rarely satisfactory to recover users active work and data recovery services, in the case of hardware failure are few and far between especially in Asia and they can never give a guarantee of success even at their high costs.

Countless notebook users learn the hard way the value of their data. From the executive whose system is stolen from a hotel room to the harried business traveller who accidentally leaves his machine in an airport departure lounge, thousands of people each year are grateful that they decided to back up their notebook's data before hitting the road. "It's one of the most important things a mobile computer user can do,"

[3] Saving Your Data -- And Your Skin [Comparison of Current Backup Options] *April 2001,* By John Edwards

http://www.laptoptravel.com/cgi -bin/lapt.storefront/3c5f47c60ac4f6182719d1626d0a06bb/Ext/LT_InfoCata log/ViewProduct/ART_BackingUp

PDA - Personal Digital Assistants are now very common in the work place and have eclipsed the simple schedul ing devices of the past to include Web access, email and a host of scaled down office applications. These devices rarely are fitted with any encryption capabilities and although for data synchronisation with a host laptop they normally require line of site to transmit using infra red since they can access the Web they must have dial out capabilities and radio wave transmition capabilities which as mention are currently not a secure means of data exchange. Because of there increased memory store and conveni ence even compared to laptops they are now frequently being called upon to carry important and at times confidential corporate data. For those IT support people puzzling over how something as big as a laptop could get lost these little devices are even more likely to disappear. Data backup on these things is only as recent as there last synchronisation and even then it is only a data backup not applications and as for anti -virus software it seems everybody has forgotten that these devices can receive email. There has already been at least one reported case of a palm virus. There is a definite conflict between the use of personal equipment interacting with company owned assets and serious considerate needs to be given to deciding how best to control this, if the company owns and provides the PDA it has greater control over the security set -up and given the potential risks of having unknown devices that can link to the network the cost of the PDA may be a small price to pay for extra peace of mind.

"The Phage.936 virus was discovered by antivirus researchers at McAfee.com and Finland -based F-Secure last night. The virus erases third-party applications on infected Palm operating systems"

[4] September 22 2000, First Palm virus raises questions about security, By Stephanie Miles
http://news.com.com/2100 -1040-246085.html?legacy=cnet

Wireless networking, for the convenience and ability to stay connected while people move their computers around the office without the need to be physically attached to anything we now must start making provisions for the new wireless office. The idea is good but the technology has been developed just too far ahead of all the security concerns being resolved. There is report after report warning of the insecurities with radio frequency data transmition and the only real way to make it safer is to implement encryption as a standard for all information so now you may be forced to start dealing with the complexity of im plementing PKI which is a big project by itself. Correct installation and configuration is essential for any wireless networking but much more time should be spent evaluating the security implications before this is ever attempted. How easy will it be to coexist networked and wireless segments and what will we do with all those microwave ovens in the pantry ?

" WLANs Take Hold
Organizations are deploying wireless LANs (WLAN) in large numbers, but typical of emerging technology, implementation is out in fro nt of security. Handheld devices are inherently insecure, and the current WLAN standard, 802.11b, offers immature and inadequate security. Sensitive data is being transmitted using flawed encryption, or worse, no encryption at all."

[5] January 2002**,** WIRELESS INSECURITIES, Control mobile computing vulnerabilities before they get control of you. BY DALE GARDNER
http://www.infosecuritymag.com/articles/january02/cover.shtml

Suggested Solutions

Everything must start with sound security policies for installation, use and auditing. Teaching IT staff the proper configurations at installation and training users on the security threats and means to work safely is always the best start, prevention is better than cure.

Some say by far the most important tool against security concerns is user awareness training on essential best practices common to all types of computer equipment such as; adherence to password creation rules, regularly backing up data, maintaining up -to-date anti-virus signature files, following advisories on applying software patches should be part of an on-going awareness exercise. Equipment specific training should also be provided before release to users if at all poss ible, this should cover issues such as basic care and maintenance and any security threats unique to the individual tools. Staff may be a companies greatest asset but in security they are frequently the weakest link.

"If you don't back up your investment in security technology with an equal (and relentless) commitment to training, your employees will do more harm to your reputation than a horde of hackers"

[6] 28 Jun 2001, Employees: Your best defense, or your greatest vulnerability, By Neal O'Farrell
http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci751955,00.html

Subscribing to one of many available security advisories or access one of the many security related watchdog sites to stay in touch with the latest vulnerabilities, software patches and general security news.

[7] Try, http://www.incidents.org

Provide physical hardware anti theft devices to your staff, these come in a variety of forms but the most common include; cable locks to secure

devices to unmovable furniture which is just as relevant in the office as when travelling, reports indicate up to 40 % of laptop thefts are from in the office. Most forms of visual makings and inscribed ID tags on the machine will act as a deterrent to thieves looking for something untraceable to steel. There are also stealthy trace applications for laptops that once activated will contact a command centre to let them know what phone number or IP address the stolen machine is now at. Most of these are relatively inexpensive options but nothing beats good common sense and following the policy guidelines on mobile computing, assuming your company has one.

Authentication tech niques such as smart cards and even Biometric security including fingerprint, voice and face recognition are now available on the PC at affordable prices although you should study the performance reviews before deciding to use some of these as a standard.

Encryption software to enhance the "out of box security capabilities" of most applications is worth the effort and many of these applications are free, although make sure your backup application allows you to include encrypted files or volumes.

Personal firewalls and desktop activity monitoring applications such as anti virus software should be provided for all laptops to ensure enhanced security while not attached to a corporate network. The threat of viruses, and Trojan applications is one of the big gest concerns to network security and these can frequently be introduced when mobile devices are reconnected to the network.

[8] This gives a scorecard on the most popular Personal Firewall products and explains their best and worst features, a number o f these products are free for personal use. http://grc.com/lt/scoreboard.htm

There is a new bread of protection software available defined as "Behaviour Blocking" which can compliment the traditional anti virus applications, these do not rely on comparing code signatures and as such do not require to be constantly updated. They identify code attempting to perform actions in ways which contravene a rule base of acceptable behaviour, such as mass mailing and proceed to quarantine the suspicious code into a protected area called a "sandbox". This type of protection can greatly increase your chances of surviving worm and Trojan infiltration but is not meant as a direct replacement of anti virus software. Consideration of system performance by running both types of protection need to be reviewed but will add to your defence in depth.

"The future of computer viruses seems clear enough: ever more destructive "hybrid worms" that take advantage of software vulnerabil ities

and destroy files, leave behind holes for hackers to exploit, then scan for new victims at lightning speed.

Viruses such as last year's Code Red and Nimda are overrunning traditional antivirus software and intrusion -detection systems"

[9] 01/28/02, Behavior blocking repels new viruses, By Ellen Messmer
http://www.nwfusion.com/news/2002/0128antivirus.html

VPN (Virtual Private Network), the most secure way for out of office staff to remotely connect back to the corporate network is through VPN as it provided authenticated and encrypted transmition over the low cost public network.

"As it is most commonly defined, a virtual private network (VPN) allows two or more private networks to be connected over a publicly accessed network. In a sense, VPNs are similar to wide area networks (WAN) or a securely encrypted tunnel, but the key feature of VPNs is that they are able to use public networks like the Internet rather than rely on expensive, private leased lines. At they same time, VPNs have the same security and encryption features as a private network"

[10] What is a Virtual Private Network
http://thewhir.com/find/vpn/articles /what.cfm

Example "user mobile computing policy"

The following conditions ***shall*** apply, where ***shall*** indicates something mandatory.

All mobile computing equipment ***shall*** be registered with the IT department. Upon delivery, all devises must be submitted fo r visual identification tagging and a log created to track service history.

For laptops the corporate approved anti virus software ***shall*** be loaded along with any other approved applications. Loading of unauthorised software or freeware is strictly prohib ited.

The corporate approved hard disk encryption and personal firewall software ***shall*** be loaded.

A Bios password ***shall*** be set up on all company laptop/notebook computers by the IT department.

Only authorised and properly licensed software ***shall*** be loaded onto company computing equipment. Monitoring the use of legal software on mobile computers is the responsibility of the user.

If you have received a computer as the result of an asset transfer please make sure that the IT department has re -formatted the machine and loaded the requisite corporate software prior to your use. The existence of any unauthorised software or inappropriate materials subsequently found on the machine after receipt will be assumed to be at the users full knowledge and acceptanc e. If in doubt please consult with the IT department.

Employees must ensure that the assets for which they are responsible are used and maintained in a secure manner as recommended by the manufacturers "proper use" instructions and the advisories of the I T department . This also means that assets must be appropriately labelled, not be left in a position for security to be compromised and only used for the authorised and intended tasks.

Employees ***shall*** not use any diskette on any computer unless the diskette has been first checked for viruses using the approved virus checker.

Laptops ***shall*** not be left unsecured in the office overnight, always lock them away in a strong cupboard.

The following conditions ***should*** apply, where ***should*** indicates something is good practice.

Laptops ***should*** be carried on -board for all modes of travel, not submitted as check-in luggage.

You ***should*** close all other applications while browsing the internet, particularly any connections to corporate data systems including email.

If you intend to leave you station for an extended period you ***should*** close your connection to the internet and log off from the network.

Screensaver password ***should*** be implemented and set to activate after 10 minutes of inactivity.

When using a cell phon e you ***should*** always be alert of where you are and who is around when discussing corporate matters.

Best Practice Advisory

1. Do not subject your computer keyboard to physical punishment, such as repeatedly banging the keys,

2. Do not place heavy objects on your computer.
3. Do not allow liquids onto your computer.
4. Do not disassemble your computer. Only an authorised repair person can do this.
5. Do not scratch, twist, hit or push the surface of your computer LCD display.
6. Do not pick up or hold your computer by the dis play.
7. Do not use or store your computer where the temperature is outside the manufacturers acceptable range.
8. Do not place your computer closer than 5 inches away from any electrical appliance that generates a strong magnetic field, such as a motor, magnet, TV, refrigerator, or large audio speakers.

9. Always keep an eye on your laptop, don't expect others to watch your property. Never leave you machine unattended in open view in a car or hotel room.
10. Always back-up important data files and e-mail files regularly. Critical files should be backed up immediately but at the end of each week is a good practice, you can configure your back-up to only include new or modified files to save time. Consult your IT department for more details or assistance with this. Back-up is the responsibility of the user
11. Always check to make sure you are using the latest virus checking software regularly, this can be loaded by attaching to the network and running the latest release update. Consult your IT department for more details or assistance with this.

For useful tip on mobile computing for the business traveller, including power and communications adapter requirements globally along with other useful mobile computing topics, please see www.kropla.com and www.roadnews.com . [11] and [12]

Summary

A major part of dealing with IT security and support is all about managing expectations, finding the balance between improving productivity and maintaining security along with the ability to explain to management in terms they understand why there is a need for caution and control.

You must understand what level of security your particular company or industry expects from a set of security policies and technology deployments, not all corporate cultures will accept or appreciate a too restrictive approach if the situation does not warrant it. The key is always keeping management aware of the risks and possible consequences.

Bridging the gap between technology and b usiness language is essential if you hope to get funding for enhance security features and research,

"what will be the return on investment". Using reported security articles is often not enough to get the support you are looking for from management so you must be prepared to start by working with some low cost or freeware products to begin understanding the techniques to improve security and then use the real live results from such testing to show the needs for enhanced security within your own company.
Be careful what products you use to test security within you company and it is definitely advisable to get written permission before trying out things like password hardness testing applications.

Reference Articles and Sites:

[1] January 17, 2002, Major Ob stacles Remain To Securing Wireless Devices, By Leo Pluswick
http://www.trusecure.com/html/news/press/2002/prsecuringwireless011702.shtml

[2] February 7, 2002, What's the best Way to ensure your Notebook and (probably more important) your DATA doesn't get stolen?
http://www.notebookreview.com/security.html

[3] April 2001, Saving Your Data -- And Your Skin [Comparison of Current Backup Options], By John Edwards

http://www.laptoptravel.com/cgi-bin/lapt.storefront/3c5f47c60ac4f6182719d1626d0a06bb/Ext/LT_InfoCatalog/ViewProduct/ART_BackingUp

[4] September 22 2000, First Palm virus raises questions about security, By Stephanie Miles
http://news.com.com/2100-1040-246085.html?legacy=cnet

[5] January 2002, WIRELESS INSECURITIES, Control mobile computing vulnerabilities before they get control of you. By Dale Gardner
http://www.infosecuritymag.com/articles/january02/cover.shtml

[6] 28 Jun 2001, Employees: Your best defense, or your greatest vulnerability, By Neal O'Farrell
http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci751955,00.html

[7] http://www.incidents.org

[8] http://grc.com/lt/scoreboard.htm

[9] 01/28/02, Behavior blocking repels new viruses, By Ellen Messmer
http://www.nwfusion.com/news/2002/0128antivirus.html

[10] What is a Virtual Private Network
http://thewhir.com/find/vpn/articles/what.cfm

[11] and [12] www.kropla.com , www.roadnews.com