Global Information Assurance Certification Paper

Name:- **Stuart Mears**
Certification Attempting **GSEC Practical Assignment v1.4b**
Security Essentials CISSP 10 Domains Course
Security Essentials CISSP 10 Domains Certification

Date Submitted:- **26th August 2003**
Document Version:- **1.0**

Security Concerns in a Mobile World

Summary
With the increase in ubiquitous networks and pervasive computing devices becoming commonplace, the ability for a roaming Corporate employee to access their companies assets anytime, anyplace, anyhow is becoming a reality. But with this capability, new security issues arise that a Corporate enterprise needs to educate their employees on.

This document looks at methods of providing access to Corporate information anytime, anyplace, anyhow, and the security issues related to this looking at issues from a physical, logical, cultural, and ethical point of view.

"Calling Dick Tracy !!"
The world of science fiction has often shown the ability for somebody walking down a street, in their car, or in a plane, to be able to communicate or access information via small devices attached to themselves, either as a wrist watch ala Dick Tracy, a communicator badge ala Star Trek, or via computing devices installed within their vehicle or small enough to carry in a pocket.

With the advance in telecommunication technology, the phenomenal growth in Mobile Phone capabilities, and the ever increasing miniaturisation and increase in power of computer technology, we are already in the era of being able to have access to information, be it the Internet or a Corporate network, and be able to communicate with a person via voice or data connectivity, anytime, anyplace, anyhow across most of the Globe.

This capability brings huge potential and benefits to not only individuals but to Corporate Businesses looking to have an advantage or the most up to date information available to their employees. Imagine a sales team being able to have full knowledge of current stock levels, pricing, and special offers, or a remote team being able to communicate the latest information back to head office for dispersal through out the Enterprise so that they can get answers to questions back quickly or for other departments to react to the data supplied to gain an advantage over competitors.

There are multiple factors that bring this capability to the Corporate environment. The key drivers are the ubiquitous network, ie the underlying communication technology that provides access to the Internet or Corporate

environment everywhere a user requires it, and Pervasive computing devices, ie small or integrated devices that are capable of providing enough intelligence to allow a user to interact with them to provide relevant information on demand.

What is a ubiquitous network?
A ubiquitous network is the underlying telecommunication technology that allows a user to access the information they require wherever and whenever they need to.

10 years ago all communication channels required physical cabling to route the required data back and forth between end devices. These came in the form of co-axial cables, groups of twisted pairs of copper wire, or the good old telephone line. More recently, the usage of fibre optic technology has allowed increases in bandwidth and thereby data capabilities. And now it is commonplace in developed countries to be able to access the Internet at home using high-speed technologies such as DSL or cable modems to provide access to rich, streaming data as required.

But to provide the communication capabilities wherever a user requires it, the lack of physical cabling is a must. And therefore wireless technologies are coming to the fore.

Initial 'wireless' capabilities were provided by placing infra-red transceivers onto devices which allowed them to communicate between each other over short distances, good light conditions allowing !!!

Today though, radio networks that allow users to roam wherever they like and make telephone calls to anybody in the world cover 90% of the planet. The growth in mobile phone usage was the first phase in the ubiquitous network rollout giving the individual the ability to make and receive phone calls from where ever they are (assuming network coverage), whenever they want, and to access specially built Internet sites using WAP (Wireless Access Protocol) capabilities.

This technology is constantly moving forward, and with the release of second generation phones supporting GPRS (General Packet Radio Service), always on data connections have been made possible equivalent to tethered modem speeds along with convergence of Internet standards that has allowed for true Browser capability on GPRS devices. But it has been with the release of the third generation of mobile phone technology, that near DSL speeds and the ability to stream video and provide rich content information to the device has become a reality.

There are numerous global players pushing this technology forward, such as Vodafone, Hutchinson WP, and NTT Docomo.

But wireless based networking technology is also increasing rapidly and providing bandwidth capabilities far and beyond the capabilities of 3G handsets. The 802.11x standards, more commonly known as 'Wi-Fi' (Wireless

Fidelity), currently propose 3 specifications for high-speed data communication:-

- 802.11a provides 54Mbps capabilities over a shorter range
- 802.11b provides 11Mbps capabilities over a longer range
- 802.11g provides 54Mbps capabilities over a longer range and is compatible with 802.11b

Wi-Fi capabilities are now available for PC's, Laptops, and PDA's, and Wi-Fi hot spots are growing in number with high street chains such as Starbucks providing 802.11b access to the Internet in most of their US stores.

Other wireless solutions that are still to make a major impact to the Corporate enterprise are BlueTooth, the short range radio solution that allow devices to connect together over short distances. Initially designed to provide PAN's (Personal Area Networks), networks on your person that allow your mobile phone to talk to your headset with out the need for cables, or to your PDA to give Internet browsing capabilities, as well as to reduce the clutter around PC's and their connected peripherals, ie printers, scanners, keyboards etc. It is also being looked at by Marketers to see if it can be used to push advertisements to potential customers as they walk past stores, billboards etc.

The last remaining place where the busy executive could be guaranteed to be not contactable was during flights. This is now changing with Boeing providing, via satellite communication technology, DSL speed Internet access to every seat onboard. So the busy Exec can now receive his emails and Instant Messages during the flight direct to his own Corporate device. Already British Airways and Lufthansa are trailing this solution on transatlantic crossings.

What is pervasive computing

Ubiquitous networks are only half the story. The Corporate employee on the move needs to have physical devices that are easily carried, stored securely and can be protected from damage or theft. Pervasive devices literally need to provide capabilities anytime, anyplace, anywhere.

The original and main device used is the Laptop. Designed to be carried, with internal screens and batteries, the first of these weighed nearly the same as desktop machines are were affectionately known as 'luggables'. But with advancements in CPU, screen, and battery technology, Laptops have become near standard issue for Corporate employees on the move, with capabilities equivalent to desktop machines.

But they do have the big issue of still being fairly heavy and sizable and alternatives are being sort to provide access to specific Corporate resources. PDA's, such as Palm and Handspring, or Microsoft PocketPC powered solutions by HP, Dell etc, are now a common tool in Corporate circles and have the ability to synchronise your calendar, address book, and emails originally via being physically attached to a PC via a docking cradle, or now using Wi-Fi or dial capabilities direct to your mail server. They also allow for

bespoke Corporate applications to be developed on them so that information can be captured remotely and later synced with the master application server.

The other standard Corporate tool is the mobile phone. This, as mentioned earlier, has matured considerably to allow the user to not only make & receive voice calls, but to be able to make/receive originally basic text messaging which has now evolved to allow full multi media messaging, such as digital photos and rich content, to synchronise your address book details between phone and PC, and to access Internet sites using WAP or micro-browser capabilities.

There are now appearing, cross-over devices that combine mobile phone and PDA capabilities, that. This provides the Corporate employee the ability to connect using GPRS or Wi-Fi into their Corporate network from small discrete devices. Devices such as O2's XDA, known as the Siemens SX56 in the US, provide a full functioning MS PocketPC PDA integrated with a GPRS phone with full Internet browser and POP3 email capabilities.

Also niche products are appearing that provide the Corporate employee specific capabilities on the move. Devices such as RIM's Blackberry can be integrated into the Corporate email environment, and with a relevant airtime contract, provide a platform to receive, reply, and compose emails anytime, anyplace, any where.

The era of Dick Tracy is growing closer and closer, with both PDA and mobile phone wristwatches being made available, (Fossil provide a Palm based watch and Samsung a GPRS wristwatch phone).

But true pervasiveness is just around the corner where intelligent devices will be able to access information constantly and provide it to the user in multiple ways. The ability to have access the Internet from a moving vehicle is being offered on prestige models, fridges and microwaves are coming 'Internet' connected so that they can monitor what is consumed and re-order as well as offering potential alternate access mediums to the Corporate environment. Microsoft are investing heavily in their SPOT initiative, Smart Personal Object Technology, aimed at improving and enhancing the functions of every day objects, ie fridge magnets capable of accessing and displaying real-time news and stock prices.

Methods of Remote Access

The technology for providing the capabilities to have anytime, anyplace, anywhere access to the corporate environment is here. But there are many different methods of access to Corporate information using these devices and networks, all that have their own security concerns that nee to be controlled and limited by a Corporate.

Historically the only possible access to Corporate information remotely was by dialing into the Corporate network using modems housed within Corporate datacentres. These modems either connected direct to specific applications,

i.e. Lotus Notes, SNA gateways etc, or extended the Corporate LAN over the established call to the remote PC providing full access to the LAN, such as devices like Shiva, Cisco 2500 router family, and Microsoft RAS (Remote Access Service) servers.

Today though there are two main methods for accessing Corporate information remotely – either the Corporate network is extended out to the remote device granting potentially full access to the whole Corporate environment, or the Corporate information is exposed at the boundary between Corporate control and an untrusted access point so only certain information is accessible.

Extensions of the Corporate network as described above, have now evolved into VPN (Virtual Private Network) connections with access to the Corporate network gateway across untrusted networks provided in one of two ways – either via an MSP or ISP contract.

With an MSP (Managed Service Provider) contract, access is provided using a 'closed' network provided under contract by a Network carrier, such as AT&T or MCI, and controls potential access to the Corporate information firstly by controlling access to the MSP network, and then dependent on authorisation to that, only granting access to specific resources within the MSP network. Thereby generating a 'closed' network per Corporate client. The Corporate VPN gateway then resides at this MSP boundary as a controlled resource to which only true Corporate employees have access.

With an ISP (Internet Service Provider) contract, the remote user can either have a relationship with a Corporate provided ISP contact, or any personal ISP Internet access can be used. The Corporate VPN gateway is then exposed onto the Internet for all to gain potential access to, but controlled through authorisation under the VPN setup.

VPN's are provided by numerous underlying technologies, IPsec (Internet Protocol security) , L2TP (Layer Two Tunnelling Protocol), PPTP (Point-to-Point Tunnelling Protocol), etc, all of which work on the same underlying technique. The remote users device provides correct authentication criteria to the Corporate VPN gateway, i.e. userid/password, dynamic time-sensitive PIN's (Personal Identifying Number), X.509 certificates, etc. All data passing between the device and the gateway is encrypted using industry recognised strong algorithms that protects all Corporate information moving between them.

VPN clients are currently available for all major PC operating systems and are now appearing for PDA devices and other pervasive appliances.

The other access method is moving the Corporate information required to be accessed remotely to the boundary of the Corporate environment where it meets an untrusted network. The information can then be accessed directly by the remote device, i.e. Internet sites hosting the information accessible via authenticated browsers, authenticated applications accessing relevant

gateways exposed, ie POP3 email servers and clients, RIM Blackberry devices accessing Corporate email systems via gateways on the boundary, Lotus Notes utilising passthru replication via a boundary machine into the Corporate Lotus Domino domain etc.

By creating browser accessible Internet sites containing the required Corporate information, access to it can be achieved from any device supporting standard Internet protocols, i.e. HTTP and HTML, anyplace, anytime, anywhere, potentially with out the necessity to carry any device with them.

It allows the roaming Corporate employee to access or provide data from his Corporate Laptop dialled into an ISP, from a hotel room provided Internet connection over a pay per hour ethernet or Wi-Fi connection, from his home PC connected via Broadband, from his Wi-Fi enabled PDA during a coffee break at Starbucks, or from a pay per hour Internet café/kiosk PC.

All of these methods allow access to the same Corporate Information, all have generic security concerns, but all also have unique security issues that need to be taken into consideration by any Corporate entity looking at granting remote access to Corporate information. There are limits to the extent a Corporate can control security of physical devices used for access dependant on whether they are owned and controlled by them, but there is a mindset that can be given to the employee base so that they are aware of the potential security issues and exposures that are now placed upon them.

Security concerns and solutions for the provision of remote access to Corporate information can be classified into four categories –

Physical; Logical; Cultural; Ethical.

Ways of securing things – Physically

Whilst Pervasive devices provide extreme freedom to Corporate employees due to their small size and easy accessibility, they also open themselves up to numerous physical security issues.

Their size means that they can be easily lost or stolen, and steps need to be taken to either secure the device or the Corporate information held within it. Similarly, considerations should be made for physical security constraints to restrict access to the device should it fall into the wrong hands.

If the device is to be left for any reason unattended, it should either be locked away securely, or tethered using a recognised security cable to an immovable object.

If the device should fall into wrong hands, steps should be taken to ensure that direct access to the Corporate information stored within it is not easily gained.

All devices should require authentication prior to access. The easiest option would be for the device to be secured using a strong entropy password. That is a password that is extremely difficult to predict and contains not only at least one alphabetical characters but also one numeric character, should consist of uppercase and lower case characters, and contain special characters (£$%&*?<>) if allowed. Also single dictionary based words should be avoided since these can be easily compromised using either a dictionary or brute force based attack.

These passwords should be enabled at bootup, either at a BIOS level if possible, or before access to the device is granted, i.e. login screen. This password should be asked for continually if the device has not been used for a period of time, such as by a screen saver, as normally stipulated by the Corporate Security Policy, but recommend being between 15 and 30 minutes of inactivity.

Dependent on the content of the Corporate information contained within the device, further authentication may be required. There are now PDA devices available that contain biometric authentication capabilities. The ability to identify an individual based on recognition of part of their anatomy, i.e. voice, iris, fingerprint, face etc. The HP iPAQ HP5450 for instance contains a built in thumbprint scanner that prevents access to its contents until the user has been authenticated.

By implementing a BIOS level password it should not be able to gain access to the raw data contained on hard disk or flash RAM within the device. But if an operating system level password is used it may be possible to get access to the raw data without gaining access through the device itself, i.e. booting a Laptop from a floppy disk could still give access to the harddisk within it.

Therefore it is highly recommended that all devices either have their entire storage medium encrypted using a recognised strong encryption algorithm, i.e. RSA, 3DES, AES, such as the whole harddisk or flash ROM, ie Microsoft Encrypted File System or using PGP's (Pretty Good Privacy) DISK application. If this cannot be done, the critical Corporate information should be stored within the applications encrypted using similar algorithms, that is the text file or DB cells storing the information are encrypted. This is essential if the storage mediums within the device are removable and could be removed without the employee necessarily noticing, i.e. removal harddisks, or PDAs with memory card slots, i.e. Compact Flash or SD-RAM.

All these physical controls only work on devices owned by the Corporate entity. If, as was explained earlier, the Corporate information is exposed at the boundary of the Corporate network & the Internet and is accessible via a browser, the employee can access this data from pay per hour Internet café's/kiosks. Dependent on the configuration of devices at these locations, all pages viewed through the Browser could be cached to the PC's hardisk and therefore could be accessible by the next user. It is therefore essential that users ensure they close down Browsers at these locations to remove any in-memory caches and ensures that the usage history and disk caches are

cleared when they leave the premises. One way to help reduce exposure is if the Corporate sites are accessed over secure encrypted connections, i.e. SSL (Secure Socket Layer), since these pages do not tend to be cached by Browsers but this is dependent on configuration.

Also, if they download any documents from the Corporate site, i.e. MS Word documents, Excel spreadsheets etc, they should either be saved to removable media, ie floppy disks, or the employee should ensure they are deleted from the PC.

Ways of securing things – Logically

But physically securing the device used to access the Corporate environment is only half the battle since the information can be compromised by other means.

All Corporate information being accessed remotely, be it by network extension technology or by moving the Information to the Corporate boundary, should be accessed in a secure manner. Access to the information should only be given to strongly authenticated users and all connections should be encrypted using an industry recognised strong algorithm.

Employees should be authenticated by using at least a 3-way authentication model, something to identify them – a userid; something they know – a password or PIN; something they have – either a biometric solution as described earlier, the use of PKI (Publkic Key Infrastructure) X.509 certificates, or using specific security devices to generate a time sensitive key associated with that user such as a SecureID token or smart card. Employees are then authenticated against a Corporate security list powered by either a TACAS (Terminal Access Controller Access Control System) or RADIUS (Remote Authentication Dial-In User System) server.

Similarly to prevent the Corporate information being gained whilst it is being transferred across untrusted networks, such as the Internet, all access should be encrypted. As mentioned previously, if VPN technology is being used to extend the Corporate network this should be configured to ensure that all data transferred is encrypted, i.e. IPsec, L2TP, PPTP etc. Either X.509 certificates can be issued to all employees and can be used to aid in the setup of the encrypted tunnels and authentication of the user, but this can bring a significant management overhead in maintaining the certificates dependent on the number of remote employees. Or the secure tunnels can be setup using the underlying protocol security models, such as the use of IKE (Internet Key Exchange) and ISAKMP (Internet Security Association and Key Management Protocol) within IPsec.

If the Corporate data has been moved to the boundary for access, again this should only be provided over secure connections. If Internet Browsers are being used, all connections should be made using at least SSLv2 (Secure Socket Layer) where the X.509 certificate used by the server is validated to ensure that it is still live and that it has been certified by a recognised certificate authority, such as Verisign or Thawte. If possible SSLv3 should be

used where the remote employee has been provided their own X.509 certificate as well and this is also validated to ensure that it is still live and from a recognised certificate authority, and to validate that the server and the employee have levels of trust between them prior to any web pages being displayed to the user asking for further levels of authentication, i.e. userid and password.

If gateway devices are being used to access the Corporate information, then access to these should be secured similarly. For instance, if POP3 email access is being provided then this should be made over an SSL connection to maintain the integrity of email as it is picked up (Changes access port from 110 to 995). Similarly, if niche devices, such as Blackberry's, are issued to provide email on the move, then ensure that the secure communication capabilities are enabled.

Historically, all networking technologies by default transferred data in the clear, i.e. unencrypted. Newer technologies and protocols are now providing the means for a secure transfer mechanism within themselves and this should be enabled at all times. If Wi-Fi is used within Corporate locations to allow roaming within, the Corporate environment in no longer contained within the walls of that location. Wi-Fi by its very nature will transmit outside of these confines, and as such new 'sports' such as 'warchalking' are emerging identifying these Corporate Wi-Fi hotspots and disclosing whether they are secure or not by chalk marks on the side of buildings and web site maps of hotspots.

The first thing that should be done is a SSID (Service Set Identifier) be configured to Control access to the Wi-Fi access points. Unfortunately, SSID's are transmitted in the clear as part for the 802.11 handshaking and they in their own rights therefore need securing as well. The 802.11 protocol came with its own encryption capabilities called WEP (Wireless Encryption Protocol) but by using static keys and not using a recognised strong algorithm, deciding to develop their own, security by obscurity. Within weeks this algorithm had been cracked. To try and enhance the security of Wi-Fi connections a new security protocol is being ratified called WPA (Wi-Fi Protected Access), which uses dynamic keys and stronger algorithms.

But at least using WEP provides an element of confidentiality to wireless connections and if used with other technologies, such as VPN, can provide an extremely strong access channel. And as such, any Wi-Fi access used by a Corporate employee at public hotspots should always use either VPN or SSL connections to gain access to Corporate information.

Similarly if mobile phones or GPRS enabled PDA devices are being used, these should use similar levels of security technology such as WTLS (Wireless Transport Layer Security) within the WAP protocol based on SSL technology

But accessing the Corporate environment and having the information compromised during transfer is not the only concern for devices always

connected to untrusted networks. By being always connected, or connected for longer periods on higher speed connections, they become susceptible to being compromised by people or applications looking for weakly protected systems or who are trying to gain access to that Corporate information.

Therefore, defences should be deployed on these Pervasive devices to ensure that these attempts are thwarted or at least controlled and alerted.

All devices that connect to an untrusted network should use a Personal firewall application. This is a piece of software running on the device that sits between the network protocol software and the core operating system, and decides on whether or not the connection being attempted, inbound or outbound of the device, is allowed. These can be defined to only allow the necessary connections that the remote Corporate employee requires to gain the information he needs, ideally just web access (HTTP/HTTPS, ports 80 and 443). Products such as ZoneAlarm, Norton Personal Firewall etc are well established in the area. There are also numerous open source initiatives underway as well, such as Agnitum's Outpost product.

To help detect compromises to devices, the use of Personal Intrusion Detection applications can also be considered. Here either traffic entering or exiting the device is monitored and compared to known bad traffic patterns and the connections are closed down, or key system logs are monitored to see if core application, configuration, and data files are altered or copied in anyway. Solutions such as BlackICE or SNORT provide effective solutions.

Also to aid with detection of potential threats contained within attachments received by email or items downloaded, Virus scanners should be deployed and maintained with up to date signature patterns. No longer are PC's running the Microsoft Windows operating systems the only place where viruses thrive, the first PDA virus on PALM OS has been identified, and as such the main scanner providers are now issuing solutions for PALM's and PocketPC's, i.e. McAfee's Virusscan Wireless product.

But the key security measure for any Corporate device is its configuration and the ability to maintain it. Only those applications and services/deamons necessary for the employee to function remotely should be installed and running on the device. This thereby prevents potential doorways into the device being exposed. The user of these devices also need to be prevented from altering the way it has been configured or to add their own applications to it, thereby potentially compromising the good work done by the Corporate security team in providing secure working environments.

Ways of securing things – Culturally

Technology based solutions only provide part of the solution in maintaining security, integrity, and confidentiality of Corporate information remotely accessed or carried. The actual remote Employees need to be made aware of the potential costs brought to the Corporate should that information be compromised, by either accidental or malicious means. Costs are not

necessarily monetary penalties against that employee. Damage to Corporate image and brand, stock price, and future plans, not to mention effects to the employee's career or employment record, are all significant costs if the information obtained could provide a competitor an advantage, or shows the Corporate in a bad light.

As such, all employees that either have remote access capabilities or carry Corporate information around with them should be provided training to educate them on how to use the technology solutions provided to provide integrity and confidentiality of that data. They should also be taught security principles on when and where to use the devices and any issues they should look out for during there usage. They should also know how to report potential compromises or security leaks to support groups within the Corporate.

There should also be constant targeted communication to the employee base by the Corporate reminding them of their part in maintaining security, maintaining the necessary levels of security applications on those devices, and highlighting areas where the employee should be extremely diligent in their usage of remote devices and networks to access Corporate information.

The easiest way to do this is to provide annual updates to the Corporate Security policy, or employee Code of Conduct guidelines, and ensure that all employees acknowledge that they have read, and understand them, along with the consequences for not maintaining them. Similarly, the Corporate Security Policy should be expanded to include specific areas covering remote access, Corporate information contained within Pervasive devices, and controls on usage and alterations to those devices.

But just having Code's of Conduct, or Security Policies is no good if they are not enforced according to the rules they contain. A Governance board containing senior executives should be created so that any discrepancies against these policies can be reviewed on an individual basis and the appropriate consequences agreed. Employees must be aware that if they do breach the security controls they contain, then the appropriate disciplinary action will be taken against them.

Ways of securing things – Ethically

At the end of the day though, it is up to the individual employee to ensure that they are taking the actions as defined in Corporate Security Policies and guidelines, that device security configurations are enabled and maintained, and that they take appropriate actions to ensure the Corporate information they are receiving, sending or reading is appropriately protected.

The employee needs to be aware of compromises that could be made against them, to which they may or may not be aware off. Along with education on best practices for how, when and where to access Corporate information.

Attacks open to unprepared employees include:-

- Man in the middle / replay – Is it really the Corporate site that you are accessing or a very near clone of it that is acting as a stepping stone to the real site, capturing all data that passes through it.

- Eaves dropping – both from a local vicinity point of view over hearing/seeing what the employee is doing with the device, and from somebody sniffing the local network for unprotected traffic, i.e. using a public Wi-Fi hotspot.

- Traffic Analysis – Similar to sniffing the network, but here huge amounts of data are captured with the object of identifying weaknesses in the security used with the goal of obtaining keys to break any encryption used.

A set off user guidelines should be created and provided to all remote employees providing Do's and Don't for accessing Corporate Information remotely. Suggested content of the guidelines include:-

DO:-

- Be aware of your surroundings. Can anybody near you overlook the information you are reading on screen or eavesdrop on the conversation you are having. If so, minimise time spent reviewing the information on screen or try and minimise the viewing angle to all except yourself. If you can be overheard, do not use explicit references to the Corporate, products or competitors, use aliases, code words or pseudonyms instead.

- Check that the web site you are accessing is the one you intended to visit. Check that the URL is correct and that if HTTPS has been requested to be used, ensure that an encrypted session has been generated. Look for the padlock in the bottom right corner of the Browser window. Access should only be granted to Corporate sites using as strong an encryption key length as permitted under the country of access's law. The minimum key length should be 128 bits. Check the properties of the certificate used if in doubt to ensure it is for the correct site and issued by a recognised authority (double click the padlock). Ensure that the Browser has been set to alert if any elements of the certificate are of concern, i.e. certificate not for site visited, it has expired, not a recognised issuing authority etc.

- If you are not using your own Corporate provided device and need to download documents or files to work on, it is preferable to save them to some form of removable media if possible, such as a floppy disk, re-writeable CD ROM, or USB memory stick. By doing so, no image of its contents will be left on the non-Corporate PC. The employee must remember to retrieve the media on leaving.

- If you are not using a Corporate provided device, and are viewing Corporate information through a Browser, ensure you logout of the site when finished, and close down the Browser so that any memory

resident information is cleared, such as cookies or web pages. Ensure that the Browsers cache and history are deleted when you close it down or your time completes.

- If you need to access or send documents to colleagues or customers across untrusted networks, digitally sign the document if possible to ensure confidentiality and integrity of its contents. This can be done in most email clients using X.509 certificates, or is inherent within some systems using proprietary technology, ie Lotus Notes.

DON'T:-

- Let other people use your Corporate provided device for any reason. You do not know what they may be doing with it, malicious or not.

- Use you Corporate provided device for personal use or information. Since this is Corporate provided, they own it and can request its return at any time. Similarly, using it for personal use may compromise the security environment installed on it.

Conclusion

The mobile, roaming workforce is a reality thanks to ubiquitous networks and pervasive devices. It brings increased productivity to an Employee base that can gain access to Corporate information, anytime, anyplace, anywhere. It helps to improve Employee satisfaction by helping with their work/life balance allowing them to work when and where they want.

But by providing these capabilities, the security model of the Corporate environment is expanded further than it has ever been before, whilst still being required to provide increased protection. The whole Corporate Security model needs to be managed much tighter than ever before to protect the Corporate information from numerous untrusted networks, users, and devices.

The Corporate Security department can provide tools and multiple layers of defense to secure the Corporate information accessed. But at the end of the day, it is up to the remote employee to ensure that they protect the Company assets they are using and accessing. Simple security tools and targeted education must be provided to make it as natural and intuitive as possible.

"Calling Dick Tracy", "Beam me up Scotty", "I'll check on Google"

Bibliography

References

Ubiquitous Network Technical summit – Japan 2002, presentations,
http://www.atmforum.com/meetings/ubiquitous.html

Status of Project IEEE 802.11g ,
http://grouper.ieee.org/groups/802/11/Reports/tgg_update.htm

General 802.11 information,
http://www.80211-planet.com/tutorials/article.php/1009431

Wi-Fi Concepts and information
http://www.wi-fiplanet.com

Microsoft SPOT
http://www.microsoft.com/presspass/features/2002/nov02/11-17spot.asp

Pervasive Computing Overview
http://www-3.ibm.com/software/pervasive/index.shtml

General Security Information
http://www.securityfocus.com
http://www.counterpane.com
http://www.packetstormsecurity.org
http://www.infosecnews.com

Wi-Fi Security by Stewart S.Miller
McGraw Hill, ISBN 0071410732

The Art of Deception by Kevin Mitnick, William Simon
John Wiley & Sons, ISBN 0471237124

Last Updated: July 24th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor