



Laptop & Handheld Security

D. Colin Smith
Advances in Technology
colin.smith@advancesintech.com

Questions

- Laptop Use (Company, Home, Contractors, Guests, etc.)
- Phone Use (Company, Home, Contractors, etc.)
- Handheld Use (Company, Home, Contractors, Guests, etc.)
- What issues do you all have relative to Laptops and Handhelds in your environments?

- Physical/Access Security
- Logical/Access Security
- Data Security

Policy and Procedures

- Develop Policies and Procedures
- Train Staff Regarding Policies & Procedures
 - Staff Sign and HR Scans and Uploads document to HR System
- Consistently Follow Policies & Procedures
- Regularly Evaluate Policies and Procedures & Modify as Needed

- Laptops and Handhelds
 - Train Staff on Laptop/Handheld Policies & Procedures
 - Avoid using computer bags
 - Never leave access numbers or passwords in the device's case
 - Carry your laptop/handheld with you (do not leave your laptop/handheld in your hotel room or with the front desk)
 - Encrypt your data
 - Keep your eye on your laptop/handheld

- Laptops and Handhelds (Continued)
 - Avoid setting your laptop/handheld on the floor
 - Buy a laptop security device
 - Use a laptop screen guard
 - Try not to leave your laptop/handheld in your hotel room or with the front desk

Physical Security

- Lost/Stolen Laptop/handheld
 - Change your network password to help secure access to corporate servers
 - Report the theft to your boss
 - Report the theft to local authorities (police, etc.) and to your company's IT department
 - Report the theft to your company's HIPAA Security Officer

Physical Security/Access – Risk

- Risk
 - Loss of Device
 - Unencrypted Files/Folders
 - Encrypted Files/Folders – Temporary Files unencrypted
 - Access to Entire Drive – All Profiles stored on that laptop
 - Access – Drive accessed, laptop found – far greater security risk (key loggers, access to network security)

Physical Security/Access – Prevention

- Prevention

- Lock laptop to furniture, keep handheld on you
- Set standard BIOS password required on boot for laptops
- Enable strong password entry requirement on handheld
- Root Kit to gain administrative access to laptop
- Use Strong Passwords (even if network doesn't require)
- Use Encryption Software for HIPAA/Corporate Data
- Lock keyboards when walking away from laptop/handheld
- Use Port Lock Software (Lock USB Key Ports/Floppy Drives/RWCD-DVD)

Logical Security/Access

- The more ways the laptop/handheld can connect to the online world and other resources, the more vulnerable they are.
 - Through the Web
 - Through dial-up
 - Through VPN
 - Through CDMA, TDMA, or GSM
 - Through WiFi
 - Through Bluetooth
 - Through HotSync
 - Through Infrared

Logical Security/Access - Risk

- Risk
 - Access to Data
 - Unknown Installation of Backdoor entry, Trojans, Viruses, Malware, Keyloggers, etc.
 - Unencrypted Files/Folders
 - Encrypted Files/Folders – Temporary Files unencrypted
 - Access to Entire Drive – All Profiles stored on that laptop
 - Access – Drive accessed, laptop found – far greater security risk (key loggers, access to network security)

Logical Security/Access - Prevention

- Prevention
 - Policies & Procedures
 - Use Strong Passwords (even if network doesn't require)
 - Do not keep Passwords for PDA on Laptop or for Laptops on PDA
 - Enable Password Lockout software
 - Install a Firewall
 - Install AntiVirus Software
 - Ensure Security Patches kept current
 - Install VPN Software
 - Use Strong Encryption Software for HIPAA/Corporate Data
 - Disable unsecure wireless
 - Enable secure wireless when connected to the network
 - Use Port Lock Software (Lock USB Key Ports/Floppy Drives/RWCD-DVD)



D. Colin Smith
Advances in Technology
colin.smith@advancesintech.com