Managing the Security and Privacy of Electronic Data in a Law Office

Presented by: David Reid
February 25, 2005

Introduction
- understand some key technology risks and threats to the privacy, confidentiality, and security of your information
- identify strategies and best practices for mitigating these risks
- provide resource and reference material (* indicates site references)

Wireless
- very easy to steal unsecured signals, creating a tremendous security risk
- most new systems come with wireless NIC activated by default
- "Evil Twin" evolving as a new wireless threat
- key: seeking a balance between cost/effort and risk/vulnerability

Wireless - Where are We Today?
- current standard is 802.11i (set June 2004)*
- new version offers stronger security, but may not be compatible with older equipment or systems
- if it is compatible with old systems... will security be as strong as the weakest link?

Going Wireless? Some Tips
- ensure that security is configured*
- change the default admin password
- disable remote administration features
- do not set up an access point in an office with wired firewalls

Malware: Viruses and Spyware
- malware: a program loaded on your computer (with/without consent) that performs malicious actions
- includes viruses, worms, spyware, etc.
Viruses & Worms

- virus: software program that embeds itself in another program on your computer
- worm: virus that replicates itself
- Trojan Horse: program that purports to do one thing, but does another
- malware can combine one or more of these

Defending Against Viruses

- best defenses against viruses:
  1. install anti-virus software (e.g., Symantec or McAfee)*
  2. ensure definitions are kept up to date
  3. scan regularly
  4. take care in opening email attachments
  5. take care in downloading/running programs

Spyware Defined

- spyware: a program that covertly sends information about a computer or its use to another individual or company

Defending Against Spyware

- best defenses against spyware:
  1. install anti-spyware software (e.g., Spybot or AdAware)*
  2. ensure definitions are kept up to date
  3. scan regularly

Spam Filtering

- not just for filtering space and time wasting emails
- useful for "de-fanging" virus emails
- help prevent phishing scams from getting through

Spam Filtering Approaches

- hardware "appliances"
- software applications pre-screen emails, virus-check, quarantine, categorize (e.g., SurfControl*)
- black list subscriptions*
**Phishing**
- fraudulent emails/websites that entice you to supply personal information
- major financial institutions and retailers have been spoofed
- don't respond to requests for personal information via email*

**Windows Clean-up**
- Internet Explorer clean-up doesn't do it all!
- consider third party product to clean, anonymize web browsing (e.g., SecureClean*)
- more advanced Windows analysis tools available as well*

**Windows Patch Management**
- tough to keep up with patches, but consider the alternative...
- subscribe to alerts, use built-in Windows update utilities
- preferred setting - alert, but manually install - gives maximum control

**Windows XP - Service Pack 2 (SP2)**
- includes pop-up blocking features, centralized security, and a basic personal firewall
- evaluate carefully before upgrading to the next service pack
- make a backup!

**Windows XP - Service Pack 2 (SP2)**
- pay close attention to older programs in terms of compatibility - some won't work
- check manufacturer recommendations on BIOS/driver updates first
- did I mention making a backup?

**Meta Data**
- "data about data" that's stored with your documents (e.g., Word, Excel, WordPerfect)
- "track changes" option may keep hidden revisions within your documents
- your "first offer" may ride along in your final draft!
Meta Data

- be sure to clear this information, or lock down in PDF format
- third-party products available to scrub meta data from your documents (e.g., CrossEyes*)
- tip - avoid “fast saves” options in Microsoft Office products

Data Storage Issues

- PC hard drives
  - prefer going with NTFS
  - now supports encryption
  - don’t encrypt Docs & Settings!!
- other hard drives
  - photocopiers, fax machines
  - iPod, flash/"thumb" drives
  - these can bear viruses too...

“Surplus” Computers

- “dumpster divers” pose a threat
- don’t throw out your computer without wiping it clean first... and just deleting isn’t good enough
- consider special software to “deep clean” your hardware (e.g., WipeDrive*)

“Surplus” Data Media

- diskettes and tapes
- CDs and DVDs
- consider the ball peen hammer method

PDA Security

- cell phones – PDA combos becoming prevalent
- password/security software add-ons available - depends on type/version of your PDA*
- varying quality – some will wipe contents after “x” unsuccessful access attempts

Computer Usage Policies

- set standards through best practice policies*
- some key components:
  - e-mailing handling
  - attachments
  - retention policies
  - Internet/email monitoring/blocking policies
  - password strength/rotation policies
- departure checklists
Laptop Security
- authentication: BIOS passwords, keycard, biometrics (thumb prints now standard on some IBM laptops)
- encryption
- NTFS
- are you bypassing the firewall?

Passwords
- good password practices are crucial:
  - length
  - mixed case / mixed characters
  - change frequency
  - avoid “password”, your name, obvious personal references
  - never mix business/personal passwords
  - please, no stickies!

Passwords
- never let Windows “remember” your password
  - creates a security hole at your computer
  - easily hackable*
- what’s your password “strength”?*
- alternatives - consider password manager software (e.g., Password Manager*)

Email Issues
- double-check spelling, tone, addresses, attachments, signature, disclaimer
- watch “reply all”
- out-of-office messages
- consider “blind-copy” option

Email Encryption
- not ready for prime time?
- only good “within” systems; recipient may not respect security settings
- PGP is a start, but not simple to implement
- third party secure mail services are available*

Firewalls
- larger firms should have corporate solutions already in place
- personal PCs/Laptops
  - software-based offering in XP SP2*
  - other third party applications available
  - having something is a must
  - systems are scanned within minutes on the Net
  - keep the software up to date!
Windows XP SP2 Firewall
- free component of SP2
- better than nothing, but has a few key limitations...
  - no outbound checking
  - trusts local "subnets"
  - may be incompatible with other firewall products

Third Party Firewalls
- recommend ZoneAlarm*
  - supports outbound blocking
  - more configurable
  - offers "learning" mode, backups
  - part of Integrity Enterprise suite
- another solid option: Black Ice Defender*

“Harden” Your Computer Area
- restrict access to computer, computer room
- power conditioning bar, UPS
- smoke detector
- networked temperature sensor (TempTrax*)
- secure laptop cables
- keep equipment off the floor (static/dust)
- “clean agent” fire extinguisher, sprinklers

If You Do Nothing Else...
(part 1)
1. Install Windows Critical Updates
2. Run and keep security programs updated
3. Scan for viruses, spyware, and security holes
4. Develop security and appropriate use policies
5. Use hardware or personal firewalls

If You Do Nothing Else...
(part 2)
6. Use “Good Pa$$w0rdz”
7. Remove meta data from files
8. Back up often and store off-site
9. Harden your environment
10. Harden your wireless configuration

Managing the Security and Privacy of Electronic Data in a Law Office

Questions & Answers
References

Windows/PC clean-up/analysis utilities
- SecureClean - clean user history www.whitecanyon.com/securelean_buy.php
- HiJackThis - assess programs running on your PC - www.limewire.com
- WipeDrive (formerly CleanDrive) - completely clean your old hard drive - www.accessdata.com

Firewalls
- ZoneAlarm - www.zonelabs.com
- BlackIce - blackice.iss.net

Anti-Virus
- McAfee - www.mcafee.com

Temperature Monitor:
- sematronics.com/products_temperature_monitor.php

References

Passwords
- Password Hacker - www.seepassword.com
- Password Manager - www.cp-lab.com

"Secure" Third Party Email
- www.hushmail.com
- www.ziplip.com

Anti-Virus
- McAfee - www.mcafee.com

Temperature Monitor:
- sematronics.com/products_temperature_monitor.php

References

Computer Use/Security Policies
- www.lawsociety.bc.ca/services/Practice/docs/HomeBusiness-OfficeServer.pdf
- www.infosyssec.net/infosyssec/secpol1.htm

Security Troubleshooting & Tips
- www.lawpro.ca/lawpro/Computer_troubleshooting.pdf
- www.stayasafeline.org

Meta Data
- More background - www.lawpro.ca/lawpro/meta_data.pdf

Microsoft - support.microsoft.com/default.aspx?scid=kb;en-us;223395
- WordPerfect - http://tinyurl.com/6hd24
- CrossEyes (remove Microsoft Meta data) - www.levitjames.com/crosseyes/CrossEyes.html

References

Spyware
- Spybot - http://www.safer-networking.org
- Ad-Aware - http://www.lavasoftusa.com

Microsoft Windows XP - Service Pack 2 (SP2)
- SP2 "Home Page" - http://www.microsoft.com/windowsxp/sp2/default.mspx
- Hardware/Software compatibility - http://support.microsoft.com/ssp2swenh

Spam Filtering
- SurfControl - http://www.surfcontrol.com
- SpamCop - http://bl.spamcop.net

Phishing
- Phishing alerts - http://www.millersmiles.co.uk

References

Wireless Security Articles

Security Troubleshooting & Tips
- hacking article - http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

802.11i Technical Articles
- http://www.sans.org/r/tгла/INDEX.PHPl?id=1407

Suggested Reading

PDA Security Issues

802.11i Technical Articles
- http://www.sans.org/r/tгла/INDEX.PHPl?id=1350

802.11i Technical Articles
- http://www.sans.org/r/tгла/INDEX.PHPl?id=1407

Suggested Reading

FBI Security Issues

Threats to Other Devices
- Bluetooth virus threat - http://antivirus.about.com/od/winlessthreats/a/cabir.htm


USB devices - http://www.pcmag.com/article2/0,1759,1557504,00.asp