

Safeguarding Your Firm's Technology

David J. Bilinsky

daveb@thoughtfullaw.com

Pierre-Guy Lavoie

pglavoie@sekcore.com

Constantine Karkaliotis

Constantine_Karbaliotis@symantec.com

Make this Session a Hit



- **What areas must be touched upon to make this a hit?**
- **What burning issues do *you* need addressed?**
- **This session is driven by YOU!**

Introduction

Viruses

Identity Theft

Spyware

Spam

Trojans

Malware

*** * HaCker^{Rs} * ***

Definition of Security

- “The state of being free from unacceptable risk”
- Categories:
 - Confidentiality of Information
 - Integrity of data
 - Assets
 - Efficient and Appropriate Use
 - System Availability
- The potential causes of loss are “threats” to system
“vulnerabilities”
- We are looking at how to protect yourself against these threats.



Essential Security Steps

1. Learn about computer and internet security and how to test your system.
2. Install the latest versions of browsers
 1. Internet Explorer with service pack 2;
 2. Firefox version 2.0.0.7
 3. Apple's Safari version 3
3. Harden your passwords and password security.



Essential Security Steps

4. Install and update good anti-virus, anti-spyware, anti-malware and internet security software and keep it up to date.
5. Install a firewall on your system and test it.
6. Be careful and watch for email attacks.



Essential Security Steps

7. Learn about metadata and use a metadata scrubber before sending out any documents.
8. Harden your internet and wireless connections.
9. Safely surf the web – using virtual machines and other tools.

```
<titlStmnt>
<titl>Survey for Rural Economies, 1998</titl>
<IDNo>7856</IDNo>
</titlStmnt>
<fundAg>Countryside Agency</fundAg>
<fundAg>Department of the Environment, Transport and the
Regions</fundAg>
<copyright> Social Research Centre</copyright>
<grantNo>3289460</grantNo>
<distStmnt>
<distrbtr abbr="UKDA" affiliation="University of Essex, Wivenhoe Park,
Colchester, Essex, England, CO4 3SQ">UK Data Archive</distrbtr>
<depositr>National Centre</depositr>
<depDate date="2000-05-08"/>
<distDate date="2000-06-08"/>
</distStmnt>
<keyword>ACCESS TO COUNTRYSIDE</keyword>
<keyword>AGRICULTURAL DEVELOPMENT</keyword>
<keyword>AGRICULTURAL PRODUCTION</keyword>
<keyword>AIR POLLUTION</keyword>
<keyword>COUNTRYSIDE</keyword>
<keyword>ENVIRONMENTAL CONSERVATION</keyword>
<nation>Great Britain national</nation>
<geogCover>GREAT BRITAIN</geogCover>
<geogUnit>(A)Wards; (B)Standard Regions; (C)Postcode Sectors;
(D)Parliamentary Constituencies; (E)Local Authority Districts; (F)Counties;
(G)Scottish Regional Councils</geogUnit>
```

Essential Security Steps

10. Change default settings that can expose you to threats.
11. Adopt an Authorized Use Policy.
12. Backup your data regularly.



Learn and Test

- Forewarned is forearmed
- Bruce Schneier – CTO
Counterpane Security
- www.schneier.com/crypto-gram.html
- Steve Gibson – Gibson Research Corp
 - www.grc.com – ShieldsUp!, “Perfect Password Generator”, LeakTest
- Norton Security Check
- <http://security.symantec.com>



ShieldsUP!![™]

More than 52,333,838 shields tested!

leg@l

Security Updates

- Microsoft “Check for Updates” using IE (not Firefox or Safari). (updates and patches)
- Firefox: Click on “Help” in the Menu Bar and then “Check for Updates”.
- If you are hit with malware that your AV cannot remove:
- www.spywarewarrior.com/uiuc/soft6.htm.

The Spyware Warrior Guide to

Anti-Spyware Programs:

Feature Comparison

Security Updates

- SANS Organization has tips on how to harden your system (www.sans.org)
- Check your software against their lists
- For example, there is an extensive section on hardening Internet Explorer.

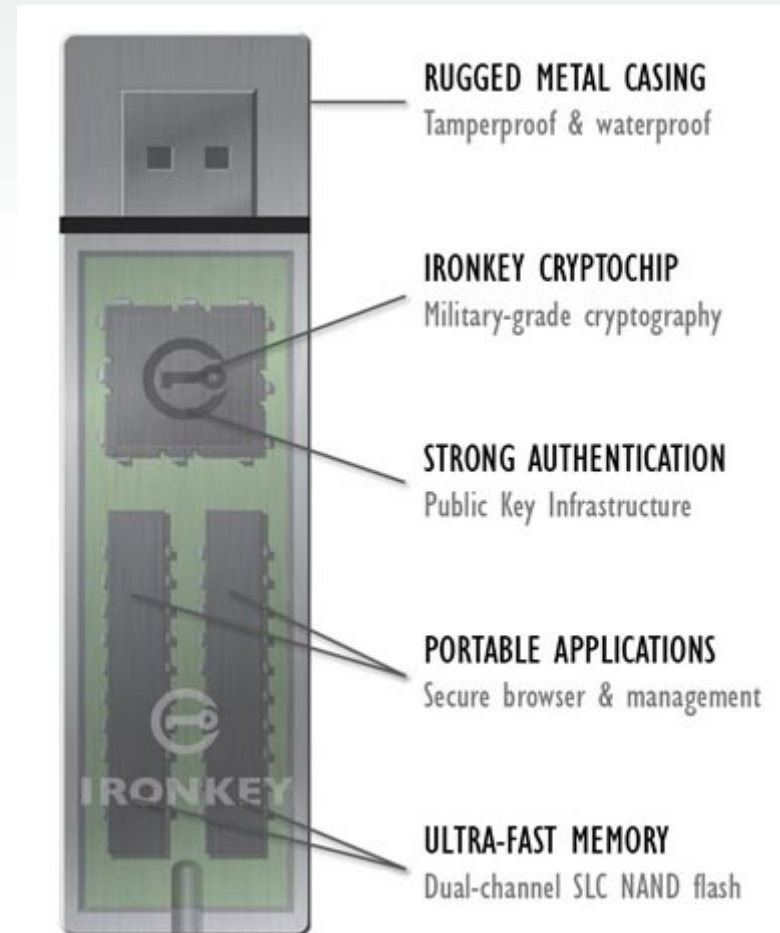
SANS NewsBites

SANS NewsBites is a semiweekly high-level executive summary of the most important news articles that have been published on computer security during the last week. Each news item is very briefly summarized and includes a reference on the web for detailed information, if possible.

Spend five minutes per week to keep up with the high-level perspective of all the latest security news. New issues are delivered free every Tuesday and Friday.

Passwords and Encryption

- What do laptops, CD-ROMs, DVDs, USB flashdrives and external hard drives have in common?
- They can be lost or stolen while containing confidential info
- Install:
 - An encryption program (www.pgp.com) \$119.00
 - A secure USB key
 - RSA key fob security token



Passwords and Encryption

- **What do:**
 - **“Mon Cheri”, “070956”, “Montreal”, “Admin”, “Password” or a note stuck to your monitor have in common?**
 - **They are all really really bad passwords!!**
 - **Don’t store your passwords in a Word or Excel file...easily found!**



Passwords and Encryption

- Good Passwords:
 - Have upper, lower case letters and characters
 - Are not names, dates or words in a dictionary
 - Change frequently
 - Are kept *Secret*
 - ~#m1ck3yM0u5e!~

Perfect Passwords

GRC's Ultra High Security
Password Generator

63 random alpha-numeric characters (a-z, A-Z, 0-9):

8EyN1GhWtnlhSVdZM1jOmTFxMTQ15nN6U12figAdRKWhwrhSBnUps3bocCV4seG

Passwords and Encryption

Password Storage Applications:

- Logon King (www.loginking.com)
- RoboForm Pro (www.roboform.com)
- Account Logon (www.accountlogon.com)
- Password Safe - *free*
- (<http://passwordsafe.sourceforge.net/index.shtml>)
- Some allow your to store your passwords on a USB drive



Antivirus, Anti-Malware Protection

- Hit with malware...who you gonna call?
- Trend Micro's "HouseCall"
- <http://housecall.trendmicro.com>
- Free scan – tells you what it found...can then go searching for a removal tool
- www.majorgeeks.com
- SpyBot Search and Destroy (www.safer-networking.org/en/index.html)



Antivirus, Anti-Malware Protection

- SpywareBlaster
- www.javacoolsoftware.com/spywareblaster.html
- Ad-Aware www.lavasoftusa.com
- *beware* of rogue software:
- www.spywarewarrior.com/rogue_anti-spyware.htm.
- Also lists trustworthy software!



SpywareBlaster 3.5.1

Prevent the installation of spyware and other potentially unwanted software!

Firewalls

- **Software firewalls:**
- **Comodo Personal Firewall,**
- **BlackICE Defender**
- **Norton Internet Security**
- **ZoneAlarm Pro**
- **AVG Internet Security**
- **Trend Micro Internet Security**



ZoneAlarm® PRO

The most secure firewall with identity and privacy protection

Add powerful, multi-layered security to your current antivirus for more protection. Includes operating system firewall, network and program firewall, anti-spyware, identity theft protection, and much more.

Firewalls

- Hardware firewalls:
- Usually built into cable and wireless modems available from:

- Linksys
- D-Link
- Netgear
- SMC

- Gibson Research:

- “ShieldsUP!!” tests a firewall and its ability to block incoming attacks.
- “Leaktest” will check your firewall for outbound data security.
- Both are available at:
www.grc.com

Dual-Band Wireless-N Gigabit Router with Storage Link
Two radio bands for twice the bandwidth!



- ◆ Internet-sharing Router and 4-port Gigabit Switch, with a built-in, dual-band, speed and range enhanced Wireless Access Point
- ◆ Two simultaneous, separate, radio bands double your available bandwidth
- ◆ MIMO technology uses multiple radios per band to create robust signals for maximum range and speed, with reduced dead spots
- ◆ Connect a hard drive or flash-based USB storage device to allow access to your music, video, or data files from within your network, or through the Internet
- ◆ Advanced wireless security and SPI firewall for protection from Internet attacks
- ◆ [3D Product View](#)

Email Dangers

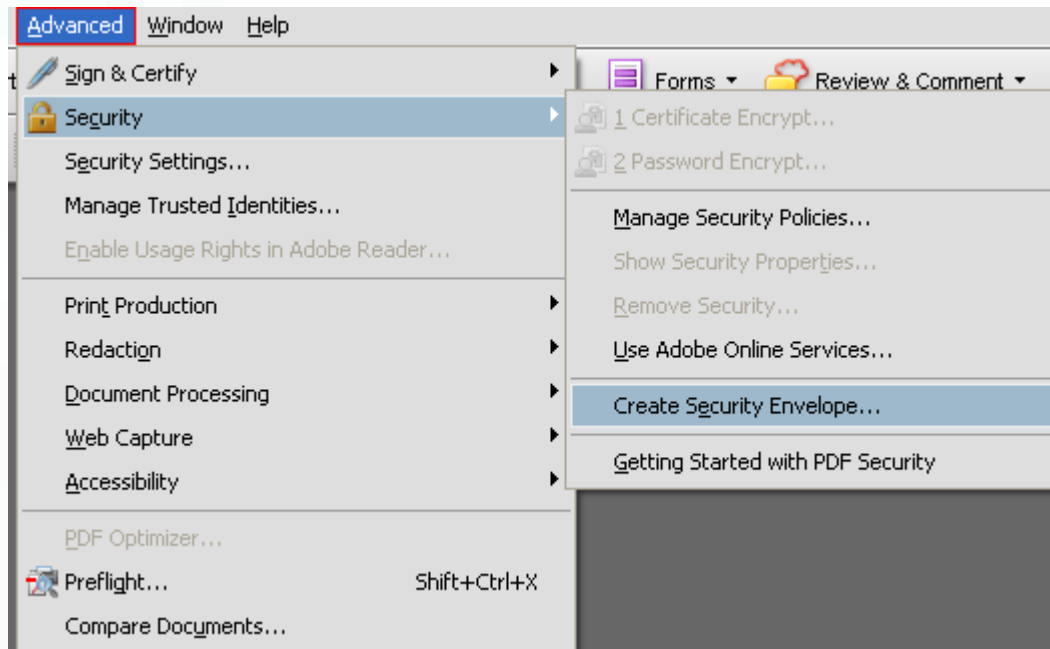
- PGP (*Pretty Good Privacy*) (www.pgp.com) for email encryption
- public/private key system
- encrypt and unencrypt email -or-

PGP Desktop Email

PGP Desktop Email: Automatic email encryption for desktops and laptops

Email Dangers

Adobe Acrobat's “password” feature:



Email Dangers

- Can be infected by opening a malicious email
- Or by following a 'phishing' email
 - IE 7 and Firefox can block or flag suspicious sites
- How to prevent Phishing:
 - Upgrade to Outlook 2003
- Install:
 - MS Office 2003 Service Pack
 - The Junk e-mail filter update for Outlook 2003



Beware of Spear Phishing!

- Highly personalized, impeccable emails (proper grammar, spelling and graphics).
- *Look* like they are from legitimate organizations (government, banks, Better Business Bureau etc).
- Install logging software on your machine - and then capture SIN, account numbers, passwords etc.



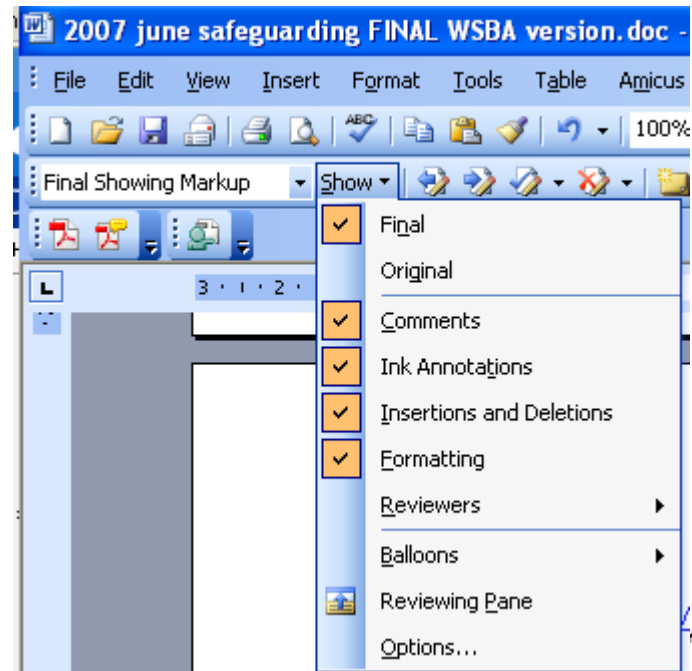
Email Dangers

- **Outlook Junk Mail Filter:**
 - Dangerous email is automatically routed to “Junk E-mail” folder
 - All formatting stripped out – all html, all pictures – only see text
 - All hypertext links are turned off
- **If good emails go in:**
 - Right-click on one of those emails.
 - Click “Junk E-Mail”
 - Then “Add Sender to Safe Senders List”

Outlook 2003 Junk E-mail Filter Update:
KB832333

Metadata

- Data hidden in the document
- Adobe Acrobat v. 8 Professional
 - ‘Examine Document’ feature
 - Determine if there is any metadata in a document and allows you to take action



Metadata

- WordPerfect offers “Save Without Metadata” feature
- Payne Consulting:
www.payneconsulting.com
 - Metadata Assistant removes metadata from Word/Excel/PowerPoint 97 and higher files

Metadata Assistant (Retail Version)



Metadata

- **Microsoft 2003+**
- **Free metadata removal tool**
- **Google Microsoft “Hidden Data Removal Tool” and install...**



Office 2003/XP Add-in: Remove Hidden Data 

Harden your Internet Connections

- **Wireless Networks**
 - Enable the strongest encryption available on the router – WPA or WPA2
- **Turn off wireless cards on laptops**
- **Don't allow wireless access points to be installed on the office network**
- **Authorized Use Policy**
- **www.lawsociety.bc.ca/practice_support/articles/docs/HomeBusiness-OfficeServer.pdf**



Surfing the Web – Safely

- **To Safely Surf – use Firefox (or Safari), not Internet Explorer**
- **Internet Explorer version 7:**
 - install all the security upgrades
 - **Securities Settings for Internet Explorer:**
 - **Disable the downloading of unsigned ActiveX controls and set “prompt” for signed ones.**
 - **Disable “Initialize and Script ActiveX Controls not marked as Safe”.**
 - **Set “Prompt” for “Run ActiveX Controls and Plugins” and “Run ActiveX Controls Marked Safe for Scripting”.**
 - **Save your changes.**



Stay Secure on the Web

Firefox continues to lead the way in online security, and now includes active protection from online scams to keep you safer.



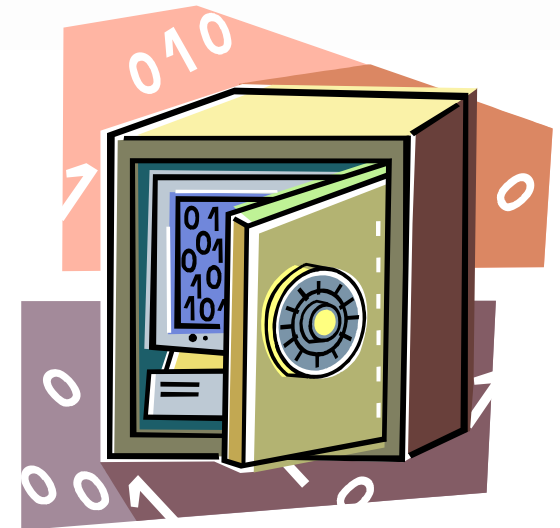
Surfing the Web – Safely

- Should be prompted when you run across a web site that wishes to run a script or ActiveX control.
- If you trust the web site, you can click ‘yes’.
- Otherwise click “No”



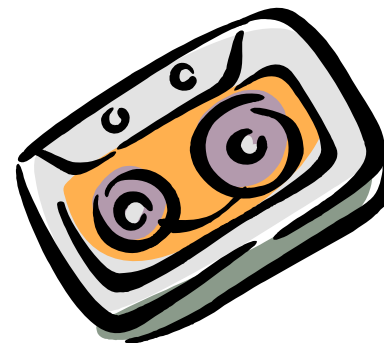
Change Default Settings

- **Disable Windows Messenger service (*this isn't Microsoft Instant Messaging application "MSN" now called Windows Live Messenger*).**
- **Change **all** default passwords**
 - Routers, computers etc...
- **Record all changes on paper and **lock up that paper****



Backups

- Good review of backup software:
- www.backup-software-reviews.com/
- Do a full backup
- Do backups daily
- Establish one person responsible for ensuring that the backups are done
- Do regular tests on the backups
- Rotate and retire tapes.
- Do an off-site backup.
- Have written instructions on how to restore the data
- Buy an external hard drive



Identity Theft and Fraud on Lawyers

- **Phishing prevention**
- **Internal fraud controls**
- **Change passwords frequently (esp after someone leaves)**
- **Bank accounts – ‘read only’ access**
- **Google yourself and your firm**



Final Tip

CCleaner

Cleans the following

Internet Explorer

Temporary files, URL history, cookies, Autocomplete form history, index.dat.

Firefox

Temporary files, URL history, cookies, download history.

Opera

Temporary files, URL history, cookies.

Windows

Recycle Bin, Recent Documents, Temporary files and Log files.

Registry cleaner

Advanced features to remove unused and old entries, including File Extensions, ActiveX Controls, ClassIDs, ProgIDs, Uninstallers, Shared DLLs, Fonts, Help Files, Application Paths, Icons, Invalid Shortcuts and more... also comes with a comprehensive backup feature.

Third-party applications

Removes temp files and recent file lists (MRUs) from many apps including Media Player, eMule, Kazaa, Google Toolbar, Netscape, MS Office, Nero, Adobe Acrobat, WinRAR, WinAce, WinZip and many more...

100% Spyware FREE

This software does NOT contain any Spyware, Adware or Viruses.



Conclusions

- **Have to take steps to harden your office against attacks**
- **Become aware of the threats and how to counter them**
- **Implement policies that counter threats**
- **Ensure your hardware, software and carbonware are up to date!~**



Questions and Thanks!



David J. Bilinsky

daveb@thoughtfullaw.com

Pierre-Guy Lavoie

pglavoie@sekcore.com

Constantine Karkaliotis

Constantine_Karbaliotis@symantec.com

SEE YOU AGAIN AT LEG@L.IT 2009 !



LAW AND INFORMATION TECHNOLOGIES

April 20 and 21, 2009
