LAW OFFICE MANAGER™
Learn More, Earn More, Be a Better Administrator

Presenter

Sharon D. Nelson, Esq. President
Sensei Enterprises, Inc.

Presenter

John W. Simek
Vice President
Sensei Enterprises, Inc.

Moderator

Catherine Jones
Online Editor
Law Office Manager

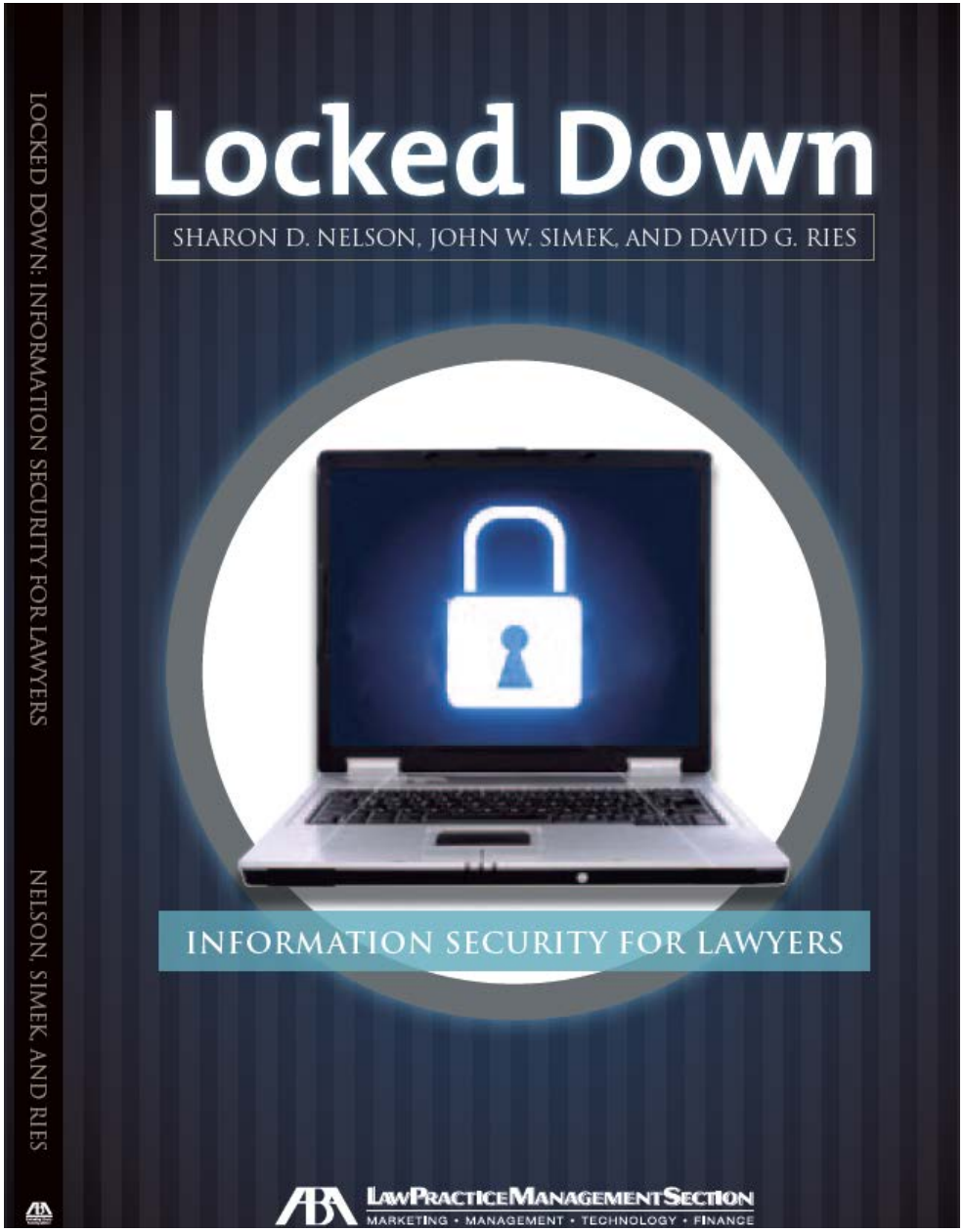
How to Protect Your Law Practice against Costly & Destructive Cyber Attack

Hot Cybersecurity Issues for Law Firms

December 10, 2014

PRESENTERS:
Sharon D. Nelson, Esq. & John W. Simek
President and Vice President, Sensei Enterprises

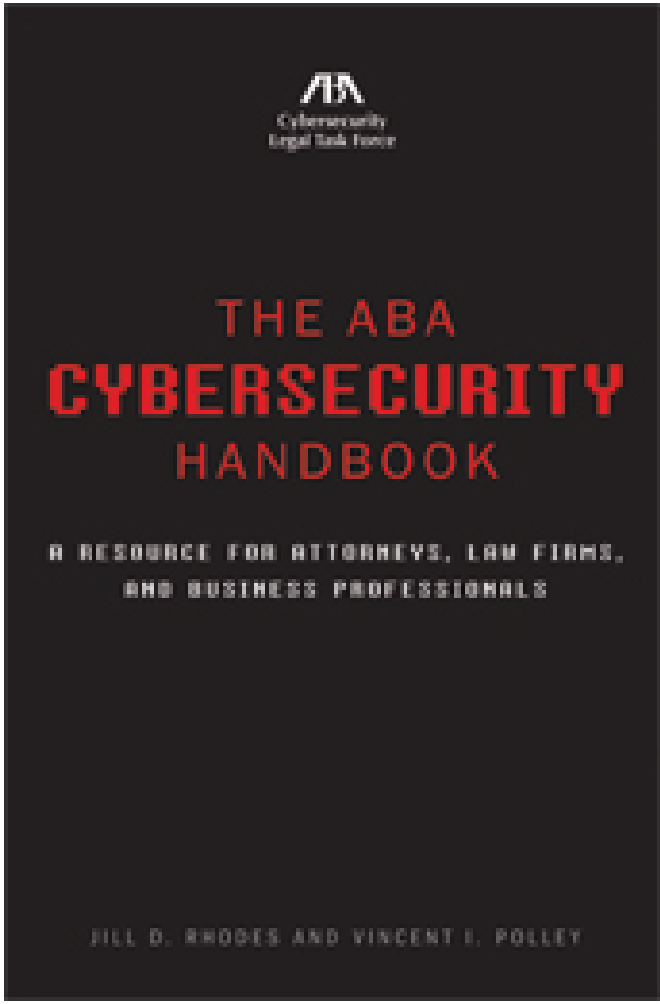
Law Office Manager


LOCKED DOWN: INFORMATION SECURITY FOR LAWYERS
NELSON, SIMEK, AND RIES
Locked Down
SHARON D. NELSON, JOHN W. SIMEK, AND DAVID G. RIES
INFORMATION SECURITY FOR LAWYERS
ABA LAW PRACTICE MANAGEMENT SECTION
MARKETING • MANAGEMENT • TECHNOLOGY • FINANCE


TRENDING
NOW

ABA Passes Cybersecurity Resolution

- August 12, 2013
- ABA's Cybersecurity Legal Task Force
- To prevent intrusions into lawyers' networks
- Foreign governments, changed to "government"
- Urges the U.S. government to work with other nations and groups "to develop legal mechanisms, norms and policies" to deter, prevent and punish such breaches




NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

What we are seeing

- More encryption
- Pre-paid untraceable phones for lawyer-client talks
- Face to face meetings – not in offices

Terrorism or economic/political espionage?

Is Skype Secure?

- Not anymore
- Microsoft has changed the rules
- 5/13/2014 – NSA can work around Skype crypto

How to meet online safely

- WebEx - Cisco
- GotoMeeting - Citrix

The FBI and law firm data breaches

- 2009 alert
- Meeting with 200 largest law firms in 2011
- Criminals, hacktivists and state-sponsored hackers
- Infected more than 8 months on average without knowing
- FBI normally alerts firms
- After notification:
  - Work with FBI and DF investigators
  - “Requests to take certain actions”
  - Remediate
  - Data breach notification laws
  - Will your insurance cover any of this?

2014 Verizon data breach report

- 60% - cybercriminals
- 25% - industrial espionage (almost all by state sponsored hackers)
- 8% - insider breaches
- First time – more breaches discovered internally than by outsiders

Wilson Sonsini – internal breach

- NY Law Journal, Sep. 17, 2014
- Senior IT employee charged with insider trading, accessed M&A files on which firm was advising
- Second breach in 4 years - an associate, also insider trading
- DLP software might have picked up “touching” of sensitive files
- Reputational damage

Wiley Rein July 2012 breach (Bloomberg news)

- Chinese hackers – Byzantine Candor
- The European Union Council, Halliburton and 18 others
- Used hidden website code – “comments”
- Other law firms also breached
- 30 researchers exploited hackers’ code to watch
- Most never spoke publicly – 3 didn’t know
- Wiley Rein said it had tightened security

Dropbox as a vehicle for data breaches?

- Claimed Dropbox data breach
- William Balaban of Stevens & Lee
- Harrisburg, PA
- Left Elliott Greenleaf & Siedzikowski
- Claim: 78,000 files synched to another computer
- Use of USB drives

Woochon William Park

- Left IP firm of Lasdas & Perry in Chicago
- Formed William Park & Associates
- Alleged he downloaded 75,000 firm files on external devices
- Third party neutral DF firm found that he deleted files at least four times after receiving litigation hold letter
- Nearly $60,000 in sanctions awarded
- IL disciplinary action

Two 2012 attempted hacks into Sensei

- Hundreds of brute force attacks in short span of time
- One from colo in Reston
- One from China
- Operated as a denial of service attack, bogging the network down
- Blocked those IP addresses
- Attempted to exploit default IDs – and in one attack, it was targeted – they knew our names

Puckett and Faraj- 2012

- Website hacked by Anonymous: “You’ve Been Owned” e-mail
- 3 GB of e-mail taken and released via BitTorrent
- Defended Marine Frank Wuterich guilty of killing 24 Iraqi civilians (the Haditha killings)
- E-mails included details from sexual assault victims
- Also, e-mail of former partner (defended Guantanamo detainees)
- E-mail hosted by website provider
- Another possible vulnerability
- Notified all clients

Law firm espionage

- West Virginia attorney figured out how another firm's attorneys accessed their e-mail (first initial, last name)
- Began spying on wife
- Moved to all the partners
- Make complex passwords

Practical Security Steps

The most common failing

- Not applying security patches or other critical updates
- Relying on outdated software for budgetary reasons – or from sheer fear of upgrading and having to learn new software!

Need to Consider ALL Data Sources

- Potential Data Sources
  - Computers
  - Smartphones
  - Flash Drives
  - External HDs
  - Servers
  - Voicemail

Employees

- Background Checks
- Internet Use Policy
- E-mail Policy
- Remote Access Policy
- Social Networking Policy
- Monitoring
- Policy Enforcement

Current Developments

- Malware Trends
  - Smartphones
  - Social Media
  - Ransomware (Cryptolocker)
  - QR Codes
  - Shortened URLs
- Apple attacks

Mobility increases security problems

- Laptops
- Netbooks
- Smartphones
- Flash Drives
- Public Computers

Secure remote access

- VPN
- Terminal Server
- Citrix
- iTwin
- Remote Control
  - LogMeIn
  - LogMeIn Ignition
  - GoToMyPC

Smartphones

- Encryption
- PIN
- Security Policy
- Remote Wipe
- Memory Cards
- Texting
- PIN-to-PIN
- iMessage

Have cell, have data, will travel

- Modern convenient devices “sync”
- What data can they sync?
- Do you have any control, by policy or other means?
- Anything that connects and can lift data must be dealt with
- BYOD
- Mobile Device Management

The Most Secure Smartphone?

1. Android
2. BlackBerry
3. Windows Phone 8
   Symbian
   WebOS
4. iPhone (now in a bendable version)

Cell phone anti-malware (iPhone and Android)

- Lookout
- Kaspersky
- McAfee
- Can’t protect iPhone’s kernel

lookout

The Only Safe Way to Fire Someone

The Terminated Employee

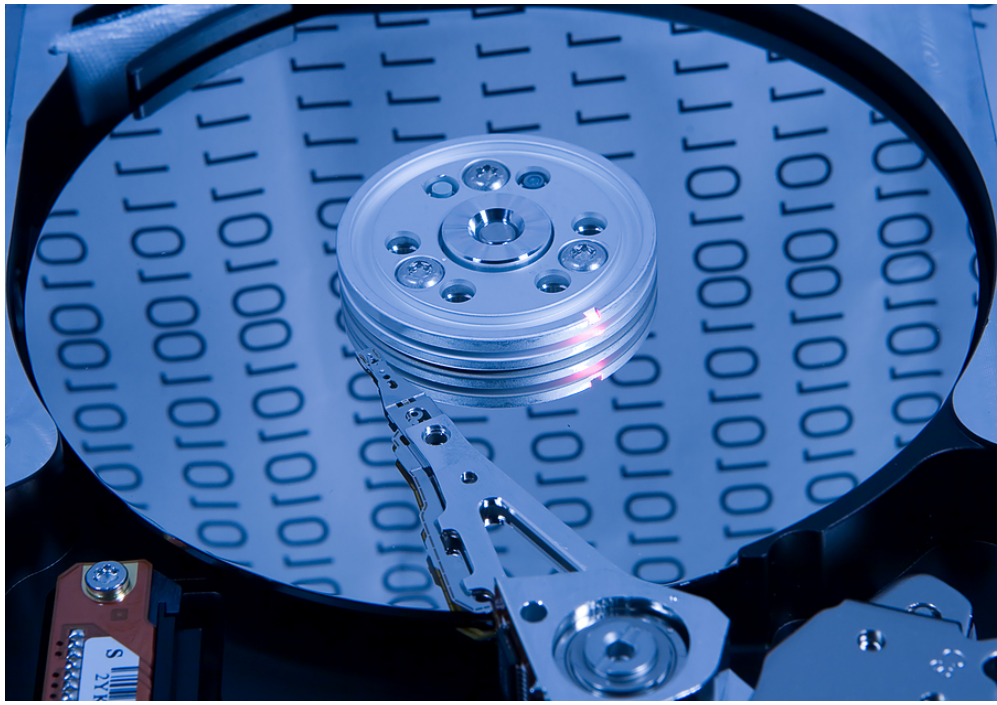
- What procedures are in place?
- No access to a computer – escort and watch if access needed
- Kill IDs
- Terminate remote access
- Mailbox terminated or forwarded to someone else

Exit Process

- Interview
- No Data Leaving
  - Get Signature that they have no data
- Employee signs statement acknowledging that access post-termination is a criminal act
- Alarm Codes
- Gather Equipment
  - Security Cards
  - Keys

Exit Process

- Email Preservation
- Computer Imaging
- DMS Logging/Tracking



What are we outsourcing?
Duty to supervise and ensure security!

- Payroll
- Virtual paralegals
- Virtual receptionists
- Backup
- Case management
- HVAC – Target breach

Cloud Computing

- Ethics
- Encryption
- Master decrypt key
- Terms of Service
- Data Location
- Exit Strategy

Cloud Services

- Dropbox
- OneDrive
- iCloud
- Google Drive
- Box
- SpiderOak

Wireless Networks

- Default Values
- Drive By
- RSA Security: 63% of surveyed networks are left at default values
- Used by Spammers
- Used by neighbors to ride your access, download porn, etc.

Wireless

- WiFi
  - Hotspots
  - WEP
  - WPA
  - WPA2
- AirCard
  - Built-In
  - Portable
- MiFi
  - Tethering

Encryption

Encryption

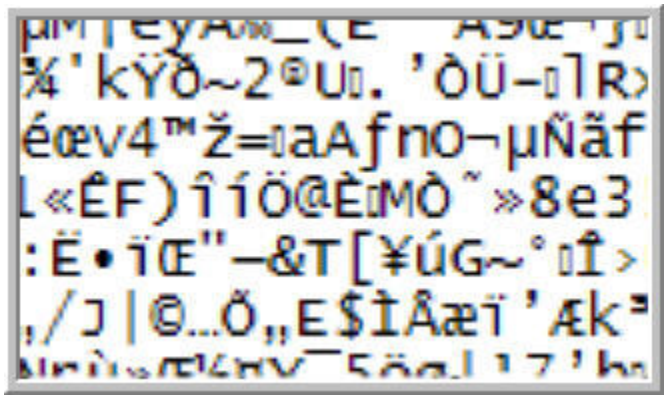
- Transmission
- Objects

Encryption

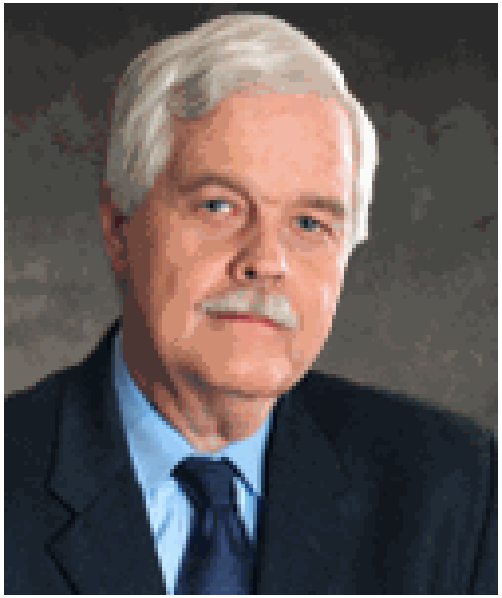
- Whole Disk
- Defined Volume
- Portable Devices
- Hardware
  - Biometrics
  - TPM
- Enterprise Admin
  - “Back Door”

Encryption Software

- Symantec Encryption (PGP)
- TrueCrypt (7.1a)
- DriveCrypt Plus
- Sophos SafeGuard
- Windows EFS
- Windows BitLocker
- Mac FileVault



Encryption Made Simple for Lawyers ALI CLE



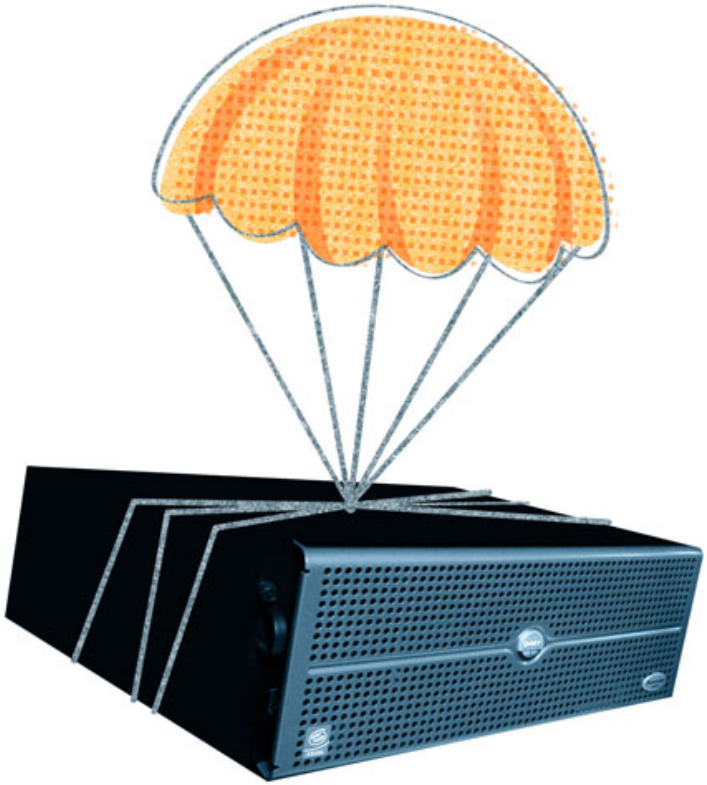
Data loss prevention software

- Set to give alerts
  - Large number of files “touched”
  - Access by non-lawyer to sensitive client data
  - Sensitive or large number of files copied or sent out of network
  - Monitoring, detecting and blocking sensitive data while **in-use** (endpoint actions), **in-motion** (network traffic), and **at-rest** (data storage)
  - Really critical documents are “tagged” for aggressive monitoring

What do first if you've been breached

- Incident response plan – lawyers, paralegals, support staff
- Call law enforcement, breach lawyer, DF experts, insurance company
- What data/clients impacted
- State data breach notification law
- May want to WATCH the hack – ID hacker, what's compromised, other means of access to network
- 3rd parties who hold your data

Backups



- Encrypted
- Multiples
- Test restores
- Synchronized
- Outsourced
  - Mozy
  - Carbonite
  - iBackup
  - i365

Software

- Anti-Virus
- Anti-Spyware
- Internet Suites
- No silver bullet
- Some will come into your network
- "Detect and respond"

Passwords – Using your pet's name? Shame, shame

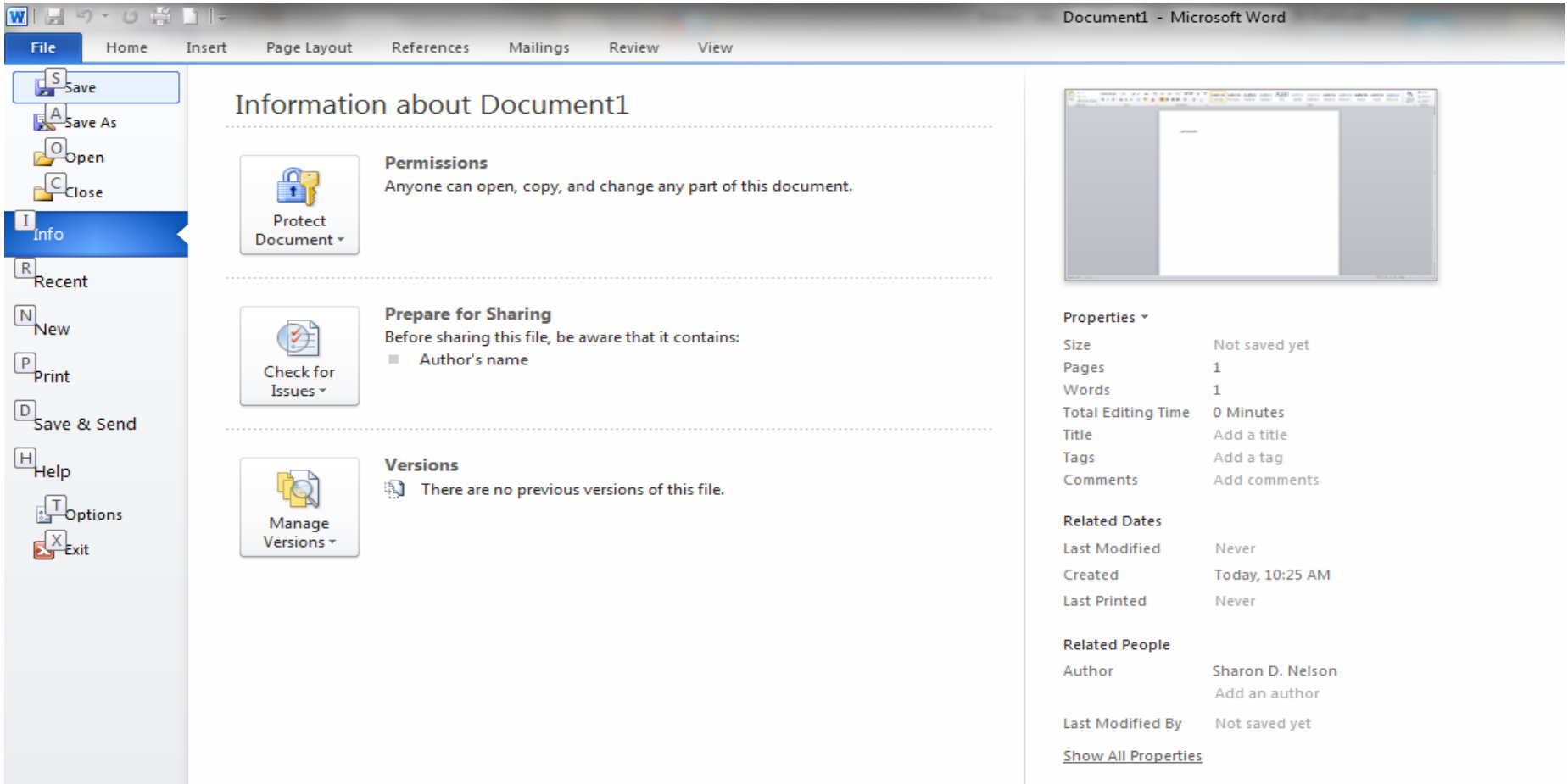
- Bella
- Strength
- Storage Location
- Power On
- Screen Saver

Password Characteristics

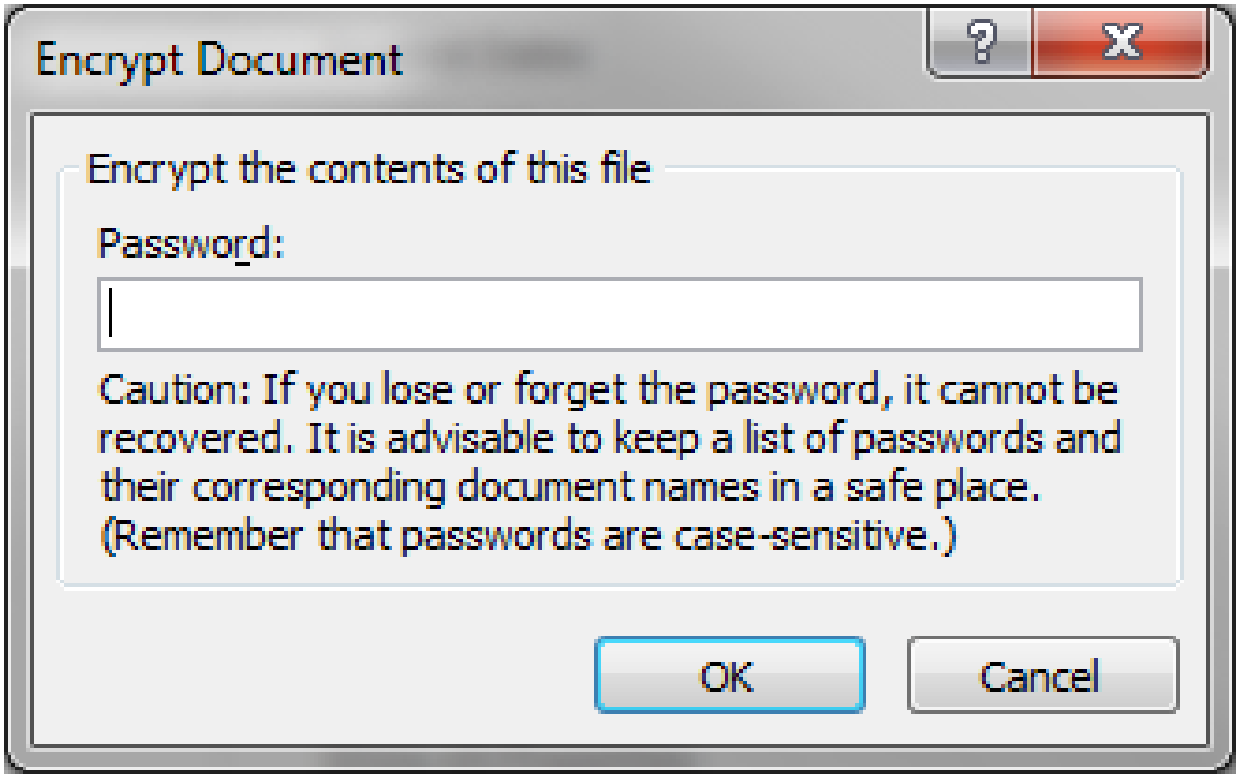
- No Dictionary Words
- U.K. – “Charlie”
- Alphanumeric
- Use a passphrase
- Length – 12 characters

How do you encrypt a document?

- You password protect it – the OPEN password
- Word or PDF – Encrypt with password



Do not send passwords in an e-mail!



Password Managers

- LastPass – free/premium version $12 a year, multi-platform
- eWallet - $19.99, $9.99 for mobile platforms
- Ironkey – hardware solution. 8 GB $199 at Walmart


ESPN
BASEBALL TONIGHT
UPDATE
FANTASY IMPACT
FREEMAN (ATL) 1-4, HR(4) 2 RBI
KEMP: 1-4 HR (12) RBI
DODGERS 2 ROCKIES 6
MIL vs SD UPDATE
DELMON YOUNG SUSPENDED
SSID: MLB-Press
Password: BWAA#2012
SSID: MLB-Photo
Password: Photo#2012
MLB
me last week after fight outside New York hotel during which police sa


SSID: MLB-Press
Password: BWAA#2012
SSID: MLB-Photo
Password: Photo#2012

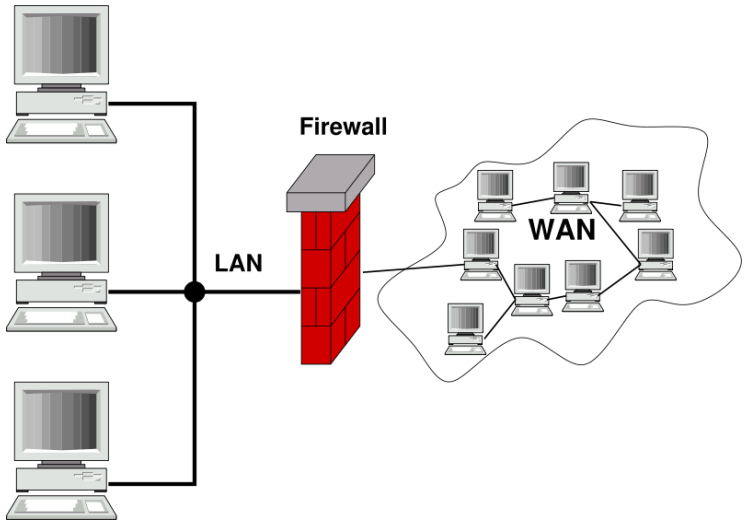

MilFlip Logon Details
Username:
Password:
ORMS
ATTENTION ALL ORMS STUDENTS


Wi-Fi Access
marko
w3Lc0m3!!!ERE
W PASSWORD *****
s case-sensitive
"Forget" or "Remove"
CBS
THIS
MORNING
SUPER BOWL SECURITY
INSIDE SECRET, FIRST-OF-ITS-KIND COM

Routers

- Defaults
- Firmware
  - Keep It Updated
- Filters
  - Enable Them

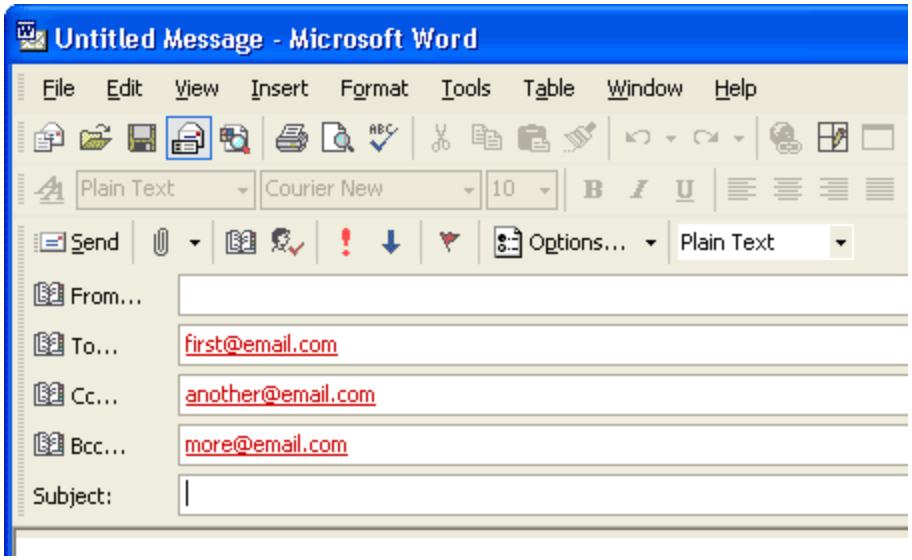
Firewall



- History
- Packet Filter
- Application Layer
- Stateful
- NAT/PAT

E-mail: Other Disclosure Dangers

- Address Books
  - Default Location
- Bcc
  - Be Careful
- Default Preview
- Typos
- Beware of Similar Names
- Distribution Lists



One Badly Misaddressed Message

Dear Lisa, I can't wait to see you tonight at the Radisson. Here's what I have planned for us, you sexy thing:

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

x

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

xxxxxxxxxxxxxxxxxxxxx

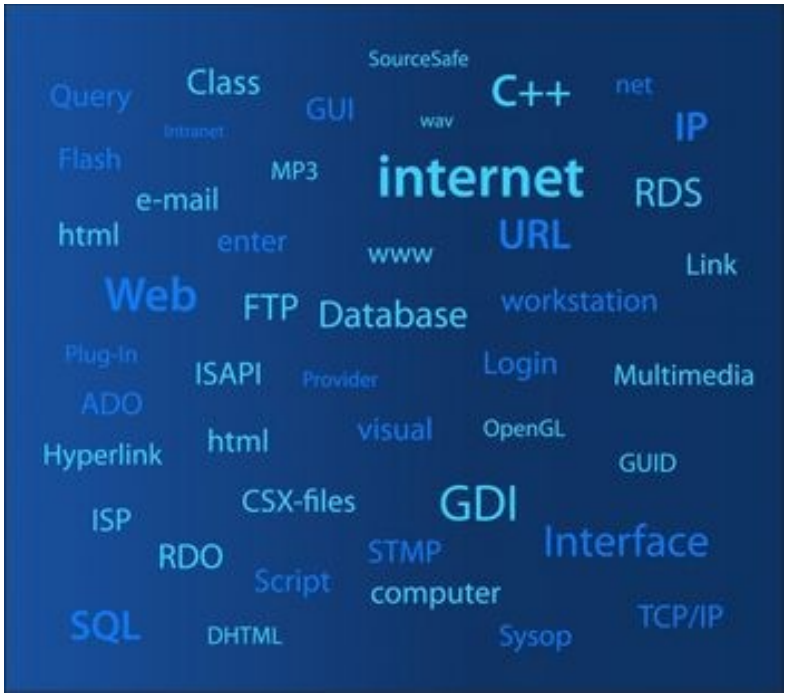
Censored!

Internet

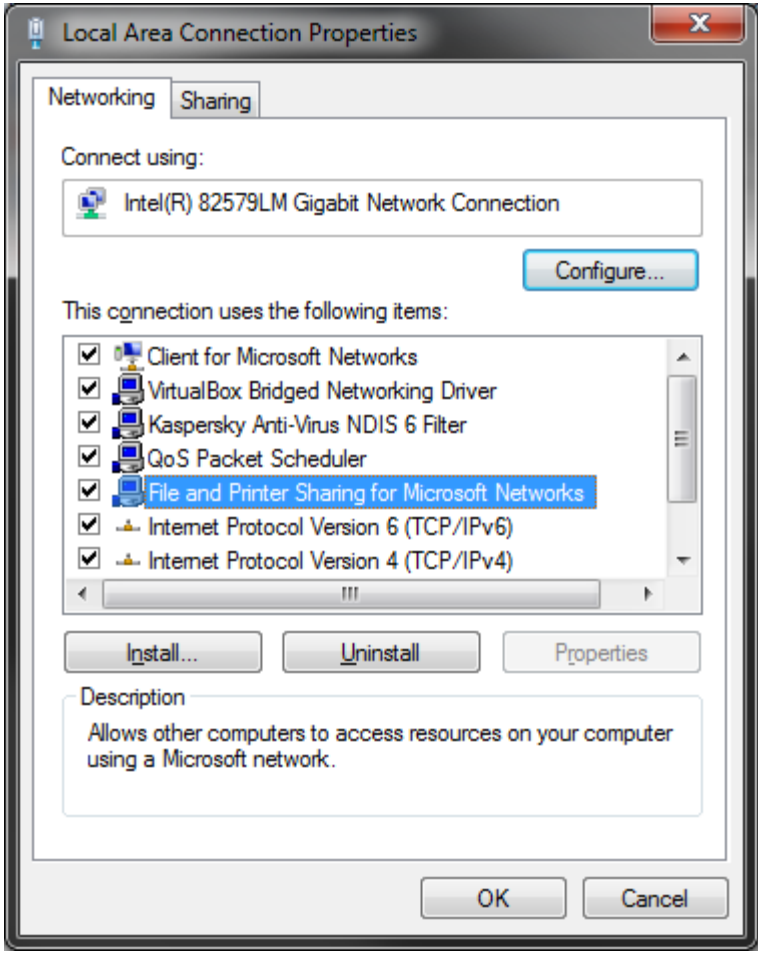
- Instant Messaging (IM)
- Spyware
- Web Browsing (Page hijack)
- Peer-to-peer (P2P)
  - KaZaA
  - Limewire
  - eMule
  - FrostWire
- Screen Savers

Internet

- Default Ports
  - 21 – FTP
  - 23 – Telnet
  - 25 – SMTP
  - 80 – HTTP
  - 5631 – pcAnywhere



File and Printer Sharing



iPods Aren't Just for Music

- Simple and looks innocent
- Are you prohibiting connections to USB ports?
- Are you logging activity if permitted?
- Under normal circumstances, you can prove access but not copying

And they love those flash drives

- Easy, fast, innocent looking
- Very portable
- All iPod remarks apply here
- Even if the use is legitimate, these things are EASY to lose
- If permitted, do you insist they be encrypted?

Equipment Disposal

- Deleted is not really deleted
- Format does not remove information
- FDISK does not sanitize
- MIT students purchased 158 disk drives on eBay
  - 74% contained recoverable data
  - 17% contained fully installed and functional operating systems
- Digital Copiers

Virtualization

- Host OS
- Guest OS
- Single Box
- Hardened

Questions?

Contact the Presenters

- snelson@senseient.com
- jsimek@senseient.com

Coming soon!

February 5, 2015

Recognizing disengaged employees

-- and how to get rid of them

Steve M. Cohen, President/Partner
of Labor Management Advisory Group, Inc. and HR Solutions: On-Call

LAW OFFICE MANAGER™
Learn More, Earn More, Be a Better Administrator

Coming soon!

March 11, 2015

Excel Essentials for the Law Office

Monica Sandler
Nation Director of Training
Attorney Resource/Dallas, Inc.

LAW OFFICE MANAGER™
Learn More, Earn More, Be a Better Administrator