

# The War Against Data Breaches



**Sharon Nelson**  
President, Sensei Enterprises  
snelson@senseient.com  
703.359.0700

**Law Office Manager**  
June 7, 2016

**John Simek**  
Vice President, Sensei Enterprises  
jsimek@senseient.com  
www.senseient.com

SHARON D. NELSON, ESQ., DAVID G. RIES, AND JOHN W. SIMEK

# LOCKED DOWN

2ND EDITION

PRACTICAL INFORMATION SECURITY FOR LAWYERS

ABA  
LAW  
PRACTICE  
DIVISION  
The Business of Practicing Law

Worried about a data breach? You should be.



# Breaches from the Am Law 200

- March 29 – *Wall Street Journal*
- Cravath Swaine and Weil Gotshall
- Breached in summer of 2015
- Other firms also breached
- Source? Unknown but CS confirmed “limited breach”
- Not aware of any improper use of info



**Weil**

CRAVATH, SWAINE & MOORE LLP



# Russian cybercriminal looking for hacker assistance

- March 29, *Crain's Chicago Business*
- “Oleras” posted in cybercriminal forum
- Offered more than \$100,000 plus 50-50 of profits exceeding \$1 million
- Insider info sought for stock market gain
- Almost 50 firms listed as targets
- A “Who’s Who” of law firms
- Two already breached – Cravath and Weil



# Data breach class action planned against elite law firms



- March 31<sup>st</sup>, *Law360*
- *Edelson PC*
- Investigated for more than a year
- Law firms (not yet named) not complying with data breach laws
- State attorneys general expected to investigate – maybe FTC

# World's largest data breach? A law firm

- April 5, *The Guardian*: “*The Panama Papers*”
- Mossack Fonseca, 11.5 million files
- 1977-present, 2.6 terabytes
- BBC – firm helped clients
  - Launder money
  - Dodge sanctions
  - Evade taxes
- Vladimir Putin – \$2 billion
- Iceland PM Gunnlaugsson resigned. Once owned – and his wife still owns – an offshore investment company with multimillion-pound claims on Iceland's failed banks



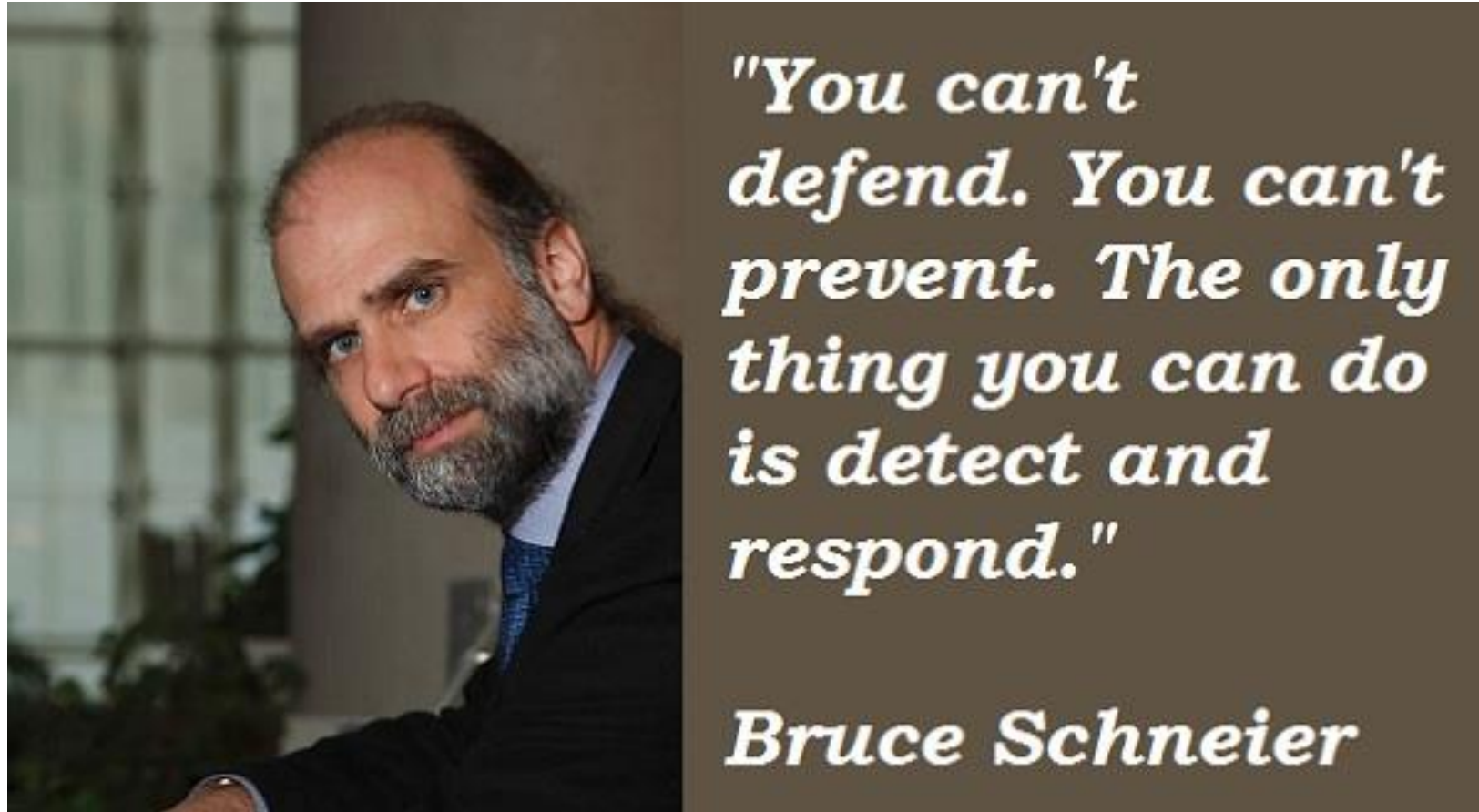
# How could such a firm be compromised?

- Their security was trivial
- An amateur could get it
- Outdated WordPress plug-in
- SQL injection vulnerability
- Website on same network as e-mail server
- Unlikely to have IDS
- On April 14, firm “raided” by government





# Advanced hackers with advanced tools



# April 12th

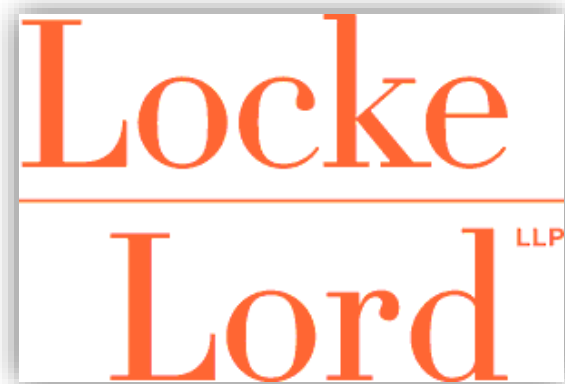
- ABA President Paulette Brown e-mail
- FBI asked ABA to transmit cybersecurity Private Industry Notifications via e-mails to its members
- 1<sup>st</sup> alert “Russian cybercriminal”
- 2<sup>nd</sup> alert: Ransomware



## ABA Cybersecurity Resolution, Aug. 2014

**RESOLVED**, That the American Bar Association encourages all private and public sector organizations **to develop, implement, and maintain an appropriate cybersecurity program** that complies with applicable ethical and legal obligations and is **tailored to the nature and scope of the organization and the data and systems to be protected.**

# Insiders: Reported 4/18/16



- Former IT engineer for a Dallas law firm
- 9 Years Prison, \$1.7 Million Fine
- Issued commands that caused "significant damage"
- "including deleting or disabling hundreds of user accounts, desktop and laptop accounts, and user e-mail accounts."

# May 9 – Second round of Panama Papers released

- Searchable by name/country
- International Consortium of Investigative Journalists
- More than 200,000 entities
- Akin Gump, Arnold & Porter, Baker & McKenzie, Bryan Cave, Dentons, DLA Piper, Greenberg Traurig, Hogan Lovells, Jones Day, K&L Gates, Linklaters, Morgan Lewis, Norton Rose, Orrick, Perkins Coie, Square Patton Boggs, Squire, Sanders & Dempsey, Troutman Sanders, White & Case, Wilmer Cutler – and the list goes on





# Panama Papers

- Whistleblowing leak
- DOJ and IRS urging folks to come forward because they are opening new investigations
- Updated list of law firms already published
- Will take months to connect all the dots and find all the beneficial owners of the shell companies



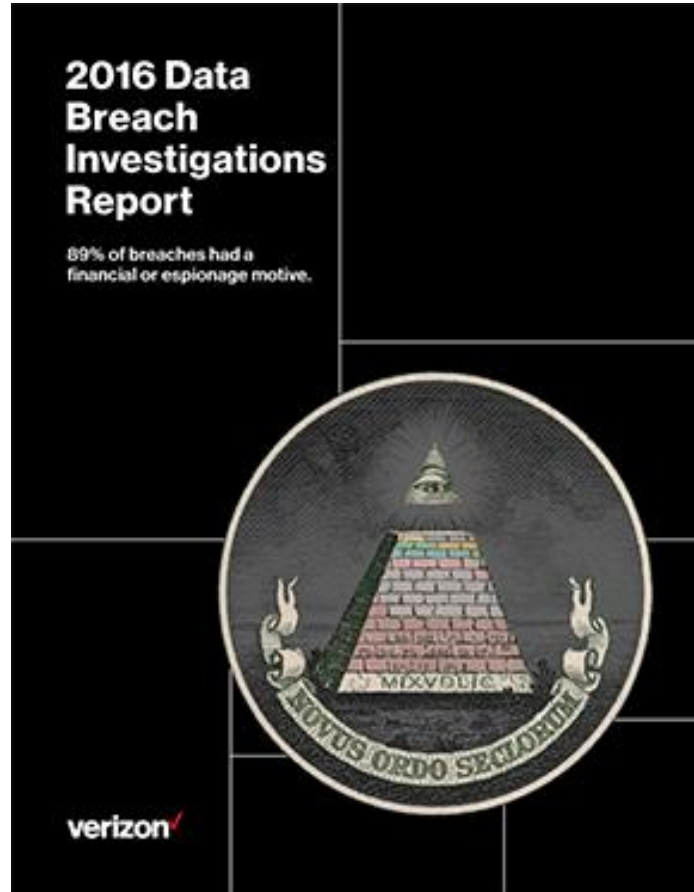
# 2016 Verizon data breach report

- Covers over 100,000 incidents, of which 3,141 were confirmed data breaches – 82 countries and many industries
- 89% of breaches had a financial or espionage motive
- 63% of data breaches involved weak, default or stolen passwords
- 30% of breaches due to human error
- 93% of breaches occurred with minutes, 11% within seconds
- Less than 25% discovered in a few days
- Bad guys have a big head start!



**“I suppose I’ll be the one  
to mention the elephant in the room.”**

# 2016 Verizon data breach report



- 30% of users opened phishing e-mails
- 12% clicked on attachment with malware or link in e-mail
- 60% of breaches happened because of phishing e-mails
- Ransomware increased 16%
- Almost as many attacks on user devices as on servers
- 80% of attacks were external

# 2015 Verizon data breach report

- By end of decade, over 5 billion IoT devices will be connected to the Internet



# The FBI and law firm data breaches

- 2016 – FBI now working with law firms through **InfraGard**
- 2009 – first alert to law firms
- Meeting with 200 largest law firms in 2011
- Infected more than 6 months on average without knowing





# Threat Actors

- Cybercriminals
- Hackers
- Hactivists
- Government surveillance
- State sponsored /  
condoned espionage
- Insiders  
(disgruntled / dishonest /  
bored / untrained)



# Law firms spending record amounts on cybersecurity

- Chase Cost Management Survey – August 2015
- Large law firms spending average of 1.9% of gross annual revenues
- AMLAW 200 – as much as \$7 million per year



# Breached Law Firms

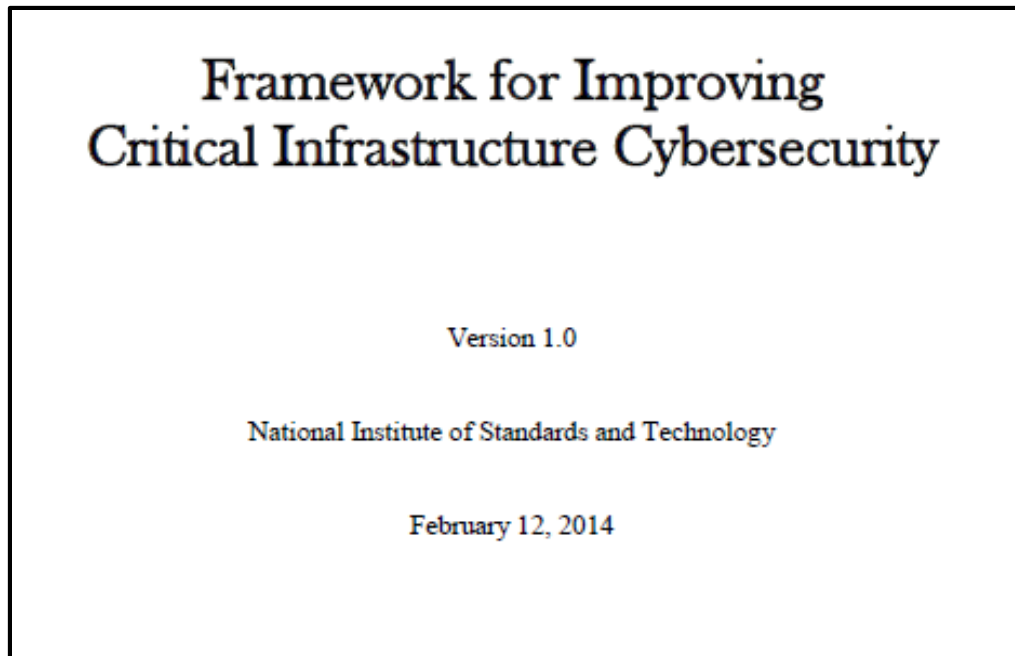
- According to Mandiant, over 80 in a single year (2011)
- 10% of work is investigating law firm breaches



# Practical Security Steps



# NIST Cybersecurity Framework: Small Business Information Security: The Fundamentals (30 pages)



DRAFT NISTIR 7621 Revision 1  
Small Business Information Security: The Fundamentals  
December 2014 – up to 500 employees  
ISO 27001



# We can't keep the barbarians at the gates

- Identify and protect – old mantra
- Now, IDENTIFY, PROTECT, DETECT, RESPOND and RECOVER



# First Five Quick Wins – Center for Internet Security

Part of the *CIS Controls for Effective Cyber Defense Version 6.0*

- Application whitelisting
- Using common, secure configurations
- Patch application software within 48 hours
- Patch systems software within 48 hours
- Reduce the number of users with administrative privileges.
- Would have prevented 85% of security incidents (Australian Signals Directorate)



# Enterprise security software

www.thaslayer.com



→ Don't know which one to choose?  
→ Check out the chart, vote in the poll.  
→ Read user opinions and suggestions.  
→ Choose the one that fits your PC the best!  
→ Share your experiences!

- Anti-Malware
- Anti-Spyware
- Internet Suites
- No silver bullet
- Some will come into your network

# Intrusion Detection Systems and Intrusion Prevention Systems

- IDS
  - Monitor inbound and outbound activity
  - Passive monitoring
  - Suspicious activity
  - Triggered actions
- IPS
  - Monitor network activity
  - Active monitoring
  - Attack behaviors
  - Automated action
  - Host-based
  - Network-based



Cisco Meraki – from several hundred dollars a year, Palo Alto Networks for larger firms



# The most common failings

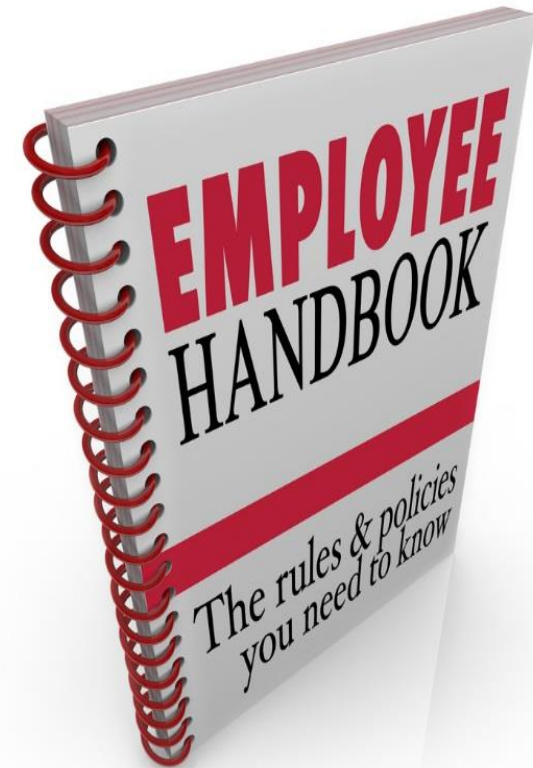
- Not applying security patches or other critical updates
- Relying on outdated software for budgetary reasons – or from sheer fear of upgrading and having to learn new software!
- Microsoft XP, Server 2003, Office 2003, IE 10 and earlier
- Apple QuickTime for Windows
- Office 2007 support ends October 2017
- Exchange 2007 support ends April 2017





# Employee Policies

- Background Checks
- Internet and E-mail Policy
- BYOD, BYON, BYOC
- Physical security
- Disaster Recovery Plan
- Encryption
- Passwords/Authentication
- Remote Access Policy
- Social Media Policy
- Incident Response Plan
  - 2015 ABA Survey
    - 28% yes
    - 47% no
    - 25% didn't know
- Monitoring and enforcement



# Incident response plan

- Templates only a starting point
- Titles of those responsible for plan functions
- Contact info – FBI regional office
  - <https://www.fbi.gov/contact-us/field/field-offices>
- Contact info – data breach lawyer
- Contact info – insurance policy (attach policy)
- Attach data breach notification law



# Incident response plan

- Contact info – digital forensics company
- Assess data compromised
- PII? HIPAA? Any other regulated data?
- Preserve system logs and DLP or IDS
- Contact info for bank
- Contact info for PR firm
- Informing employees

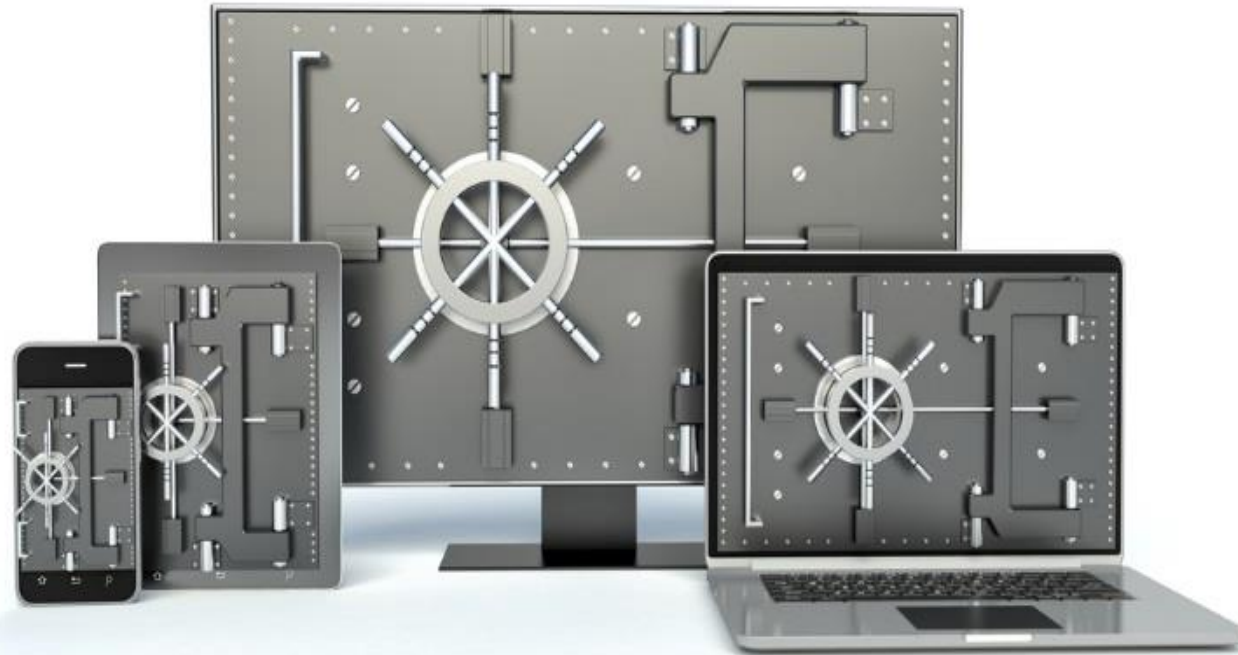


# Incident response plan

- Informing third parties
- Add and subtract issues
- Train on the plan regularly, tabletop exercises, red teams
- Annual review of plan



# Encryption



**Mother's Day**

**Graduation Celebration**

T-Shirts & Apparel

Geek Toys

Electronics & Gadgets

Home & Office

Tools, Outdoor & Survival

Geek Kids

Clearance

**SALE**

Gift Certificates

**Sign up for geek-mail**

RSS feeds

Home > Interests > Amazing Goodies >

## Rosetta Stone® - Learn to Speak Klingon



©ThinkGeek.com

[Click to zoom](#)



Let language expand your universe!

- Learn to speak Klingon today
- Live conversation sessions with native speakers
- Free, downloadable mobile companion app
- [Read more...](#)

**\$269.99** ✓ *Qapla'*

Quantity:

**BUY NOW**

or

[add to wish list](#)

Customer Action Shots:

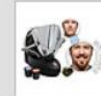


Watch the Video:



Your Fellow Smart Masses Also Bought:

Mr. Beard® Beard Machine



Unicorn Drinking Horn



[Like](#) [Share](#) < 25k

[Tweet](#) < 296

[Pin it](#) < 71

[g+1](#) < 462

**Main Description**

[Additional Images](#)





# Encryption

- Transmission
- Objects
- 2015 ABA Legal Tech Survey – only 1/3 of lawyers use encryption when sending confidential data



# Encryption



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

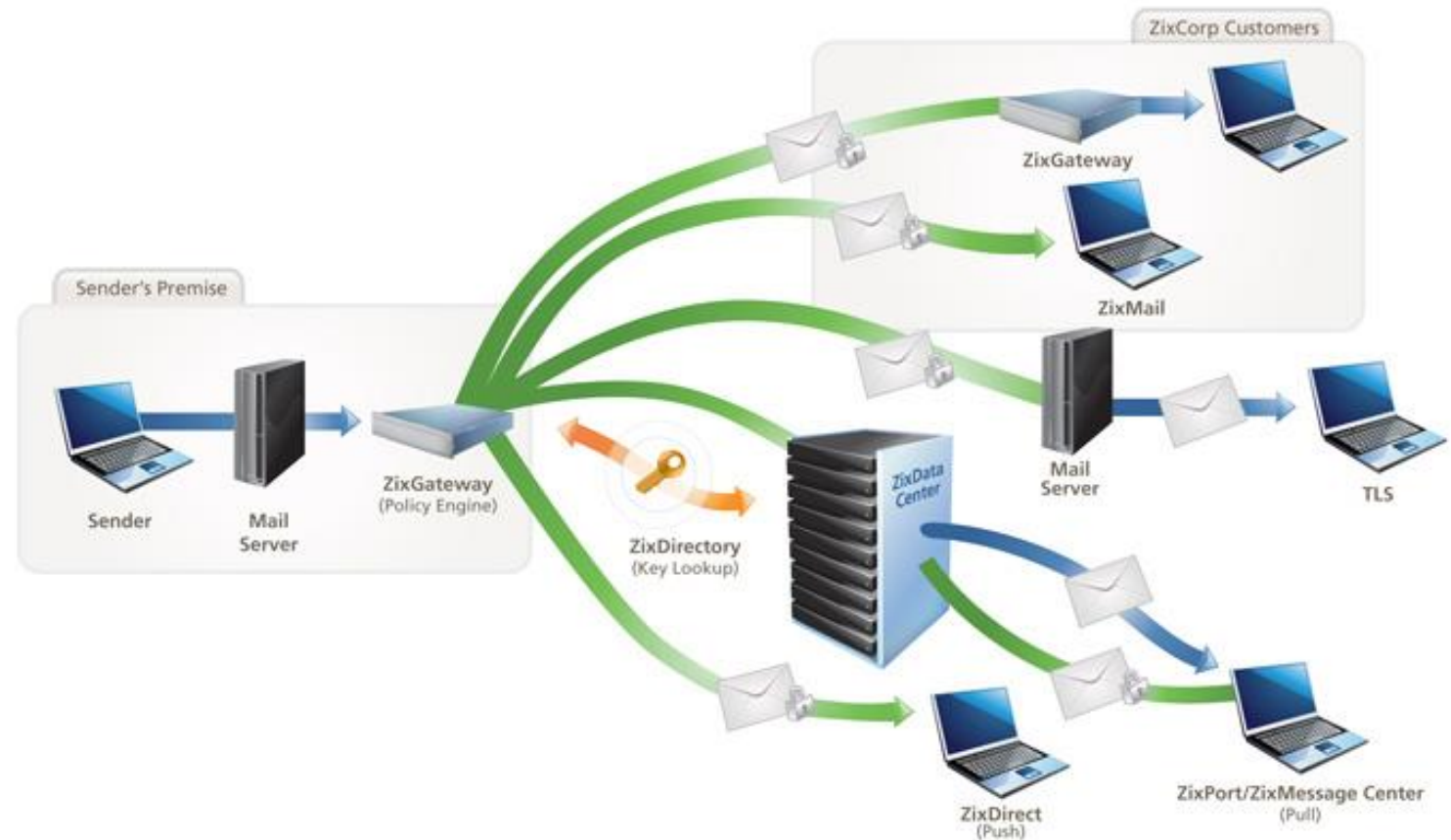
# Encryption Software

- Symantec Encryption (PGP)
- Kaspersky Endpoint Security
- DriveCrypt Plus
- Sophos SafeGuard
- Windows BitLocker
- Mac FileVault and FileVault 2



- ZixCorp
- Sophos
- Mimecast
- Proofpoint
- HP SecureMail
- EdgeWave
- Trend Micro
- Symantec
- Cryptzone
- DataMotion
- LuxSol
- Privato

# Encrypted e-mail





# The Ashley Madison breach – password lessons

Members Login ▾

**ASHLEY MADISON**<sup>®</sup>  
Life is short. Have an affair.<sup>®</sup>

Get started by telling us your relationship status:

Please Select ▾

[See Your Matches »](#)

Over **41,330,000** anonymous members!

★★★★★  
**100%**  
Like-minded  
People

**As seen on:** Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim, USA Today

Ashley Madison is the world's leading married dating service for **discreet** encounters

Trusted Security Award

**100% DISCREET SERVICE**

SSL Secure Site

[Register on Ashley Madison](#) [Affiliate Program](#) [Press](#) [FAQ](#) [Guarantee](#) [Blog](#) [Infidelity News](#) [Articles](#) [Terms](#) [Privacy](#) [Contact Us](#)

Follow Ashley Madison on: [Twitter](#) [Facebook](#) [Youtube](#)

Location: [USA](#) ▾ Language: [English](#) ▾

Ashley Madison is the most famous name in infidelity and married dating. As seen on Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim, USA Today. Ashley Madison is the most recognized and reputable **married dating company**. Our Married Dating Services for Married individuals Work. Ashley Madison is the most successful website for **finding an affair** and cheating partners. Have an Affair today on Ashley Madison. Thousands of **cheating wives** and cheating husbands signup everyday looking for an affair. We are the most famous website for **discreet encounters** between married individuals. Married Dating has never been easier. With Our affair guarantee package we guarantee you will find the perfect affair partner. Sign up for Free today.

© 2001 - 2015 Avid Dating Life Inc.

**18+ Adult Dating** means that all members must be 18 years or older

Sitemap



Who  
Wants  
To  
Hack  
Me

- 123456
- 12345
- Password
- DEFAULT,
- 123456789.
- Storage Location
- Power On
- Screen Saver



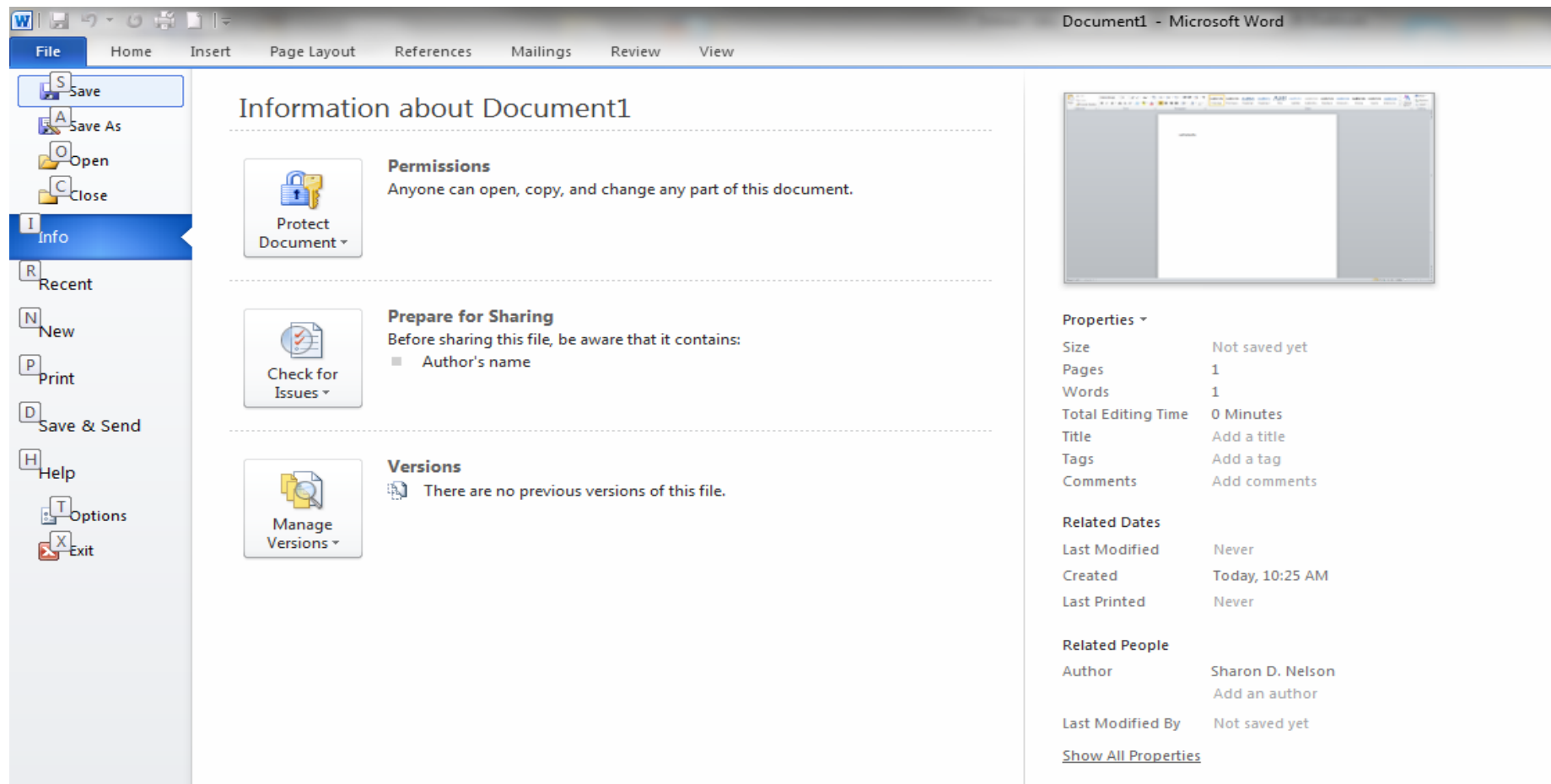
# Password Characteristics

- Still a password driven world
- No Dictionary Words
- Alphanumeric
- Upper and lower case
- Special characters
- Use a passphrase
- Length – 14 characters
- Ihavebeen-and-always-shall-be-your-friend.22715



# How do you encrypt a document?

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



The screenshot shows the Microsoft Word interface with the 'File' tab selected. The ribbon includes options for Save, Save As, Open, Close, Info, Recent, New, Print, Save & Send, and Help. The 'Info' tab is active, displaying 'Information about Document1' with sections for Permissions, Prepare for Sharing, and Versions. The 'Protect Document' button is highlighted, indicating the document is password-protected.

**File** Home Insert Page Layout References Mailings Review View

Document1 - Microsoft Word

**File** Save Save As Open Close Info Recent New Print Save & Send Help Options Exit

### Information about Document1

**Permissions**  
Anyone can open, copy, and change any part of this document.

**Protect Document**

**Prepare for Sharing**  
Before sharing this file, be aware that it contains:

- Author's name

**Check for Issues**

**Versions**  
There are no previous versions of this file.

**Manage Versions**

**Properties**

Size	Not saved yet
Pages	1
Words	1
Total Editing Time	0 Minutes
Title	Add a title
Tags	Add a tag
Comments	Add comments

**Related Dates**

Last Modified	Never
Created	Today, 10:25 AM
Last Printed	Never

**Related People**

Author	Sharon D. Nelson
	Add an author
Last Modified By	Not saved yet

[Show All Properties](#)

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
- Keeper - \$29.99 per year
- PC Magazine – best password managers -2016:  
<http://www.pcmag.com/article2/0,2817,2407168,00.asp>

**LastPass** 

The Last Password You'll Ever Need.

# Biometrics and 2FA

- Biometrics is not a good solution – once your biometrics are owned, they will always be owned (voiceprints, fingerprints, retinas) – 5.6 million fingerprints stolen in OPM breach
- 2FA is here and growing rapidly – enable wherever you can
- Best protection? Something you know, something you have and something you are



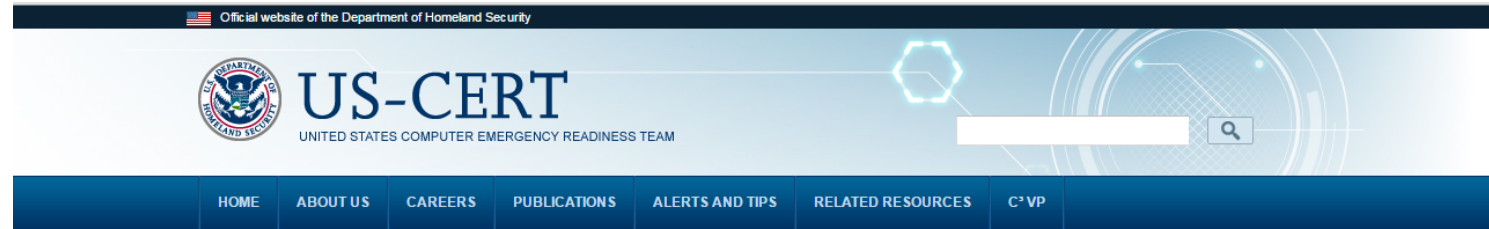
# Ransomware



- How do you get it?
- What does it do?
- How do you get your data back?
- How do you engineer backups that are impervious to ransomware?
- 4000% increase in 2014
- 165% increase in 2015



# U.S. and Canada Issued Joint Ransomware Alert, March 31



## Alert (TA16-091A) Ransomware and Recent Variants

[More Alerts](#)

Original release date: March 31, 2016

[Print](#) [Tweet](#) [Send](#) [Share](#)

### Systems Affected

Networked Systems

### Overview

In early 2016, destructive ransomware variants such as Locky and Samas were observed infecting computers belonging to individuals and businesses, which included healthcare facilities and hospitals worldwide. Ransomware is a type of malicious software that infects a computer and restricts users' access to it until a ransom is paid to unlock it.

The United States Department of Homeland Security (DHS), in collaboration with Canadian Cyber Incident Response Centre (CCIRC), is releasing this Alert to provide further information on ransomware, specifically its main characteristics, its prevalence, variants that may be proliferating, and how users can prevent and mitigate against ransomware.

### Description

#### WHAT IS RANSOMWARE?

Ransomware is a type of malware that infects computer systems, restricting users' access to the infected systems. Ransomware variants have been observed for several years and often attempt to extort money from victims by displaying an on-screen alert. Typically, these alerts state that the user's systems have been locked or that the user's files have been encrypted. Users are told that unless a ransom is paid, access will not be restored. The ransom demanded from individuals varies greatly but is frequently \$200-\$400 dollars and must be paid in virtual currency, such as Bitcoin.

Ransomware is often spread through phishing emails that contain malicious attachments or through drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge.

Crypto ransomware, a malware variant that encrypts files, is spread through similar methods and has also been spread through social media, such as Web-based instant messaging applications. Additionally, newer methods of ransomware infection have been observed. For example, vulnerable Web servers have been exploited as an entry point to gain access into an organization's network.

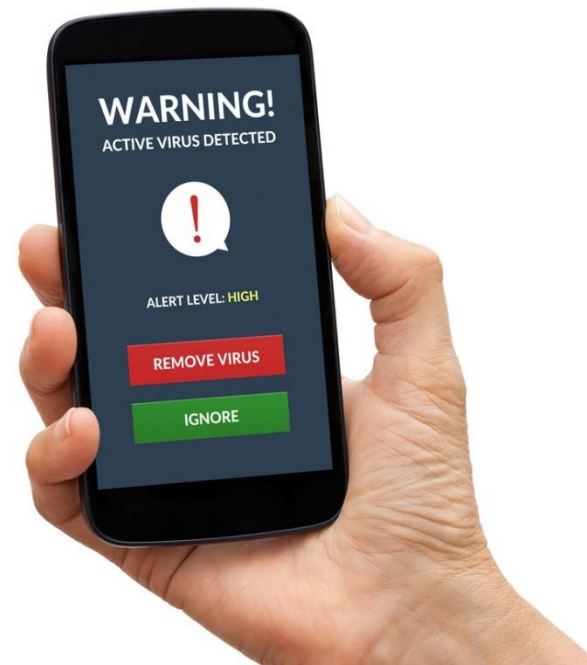
#### WHY IS IT SO EFFECTIVE?

The authors of ransomware instill fear and panic into their victims, causing them to click on a link or pay a ransom, and users systems can become infected with additional malware. Ransomware displays intimidating messages similar to those below:

- "Your computer has been infected with a virus. Click here to resolve the issue."
- "Your computer was used to visit websites with illegal content. To unlock your computer, you must pay a \$100 fine."

# Ransomware attacking mobile devices

- Began in 2015 and growing
- Downloading apps from unsanctioned app stores
- One example: SimpleLocker
  - Runs until all data on phone is encrypted
  - Sets a time limit for payment
  - No payment? All files erased



# Backups



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

# Cloud Computing



- Ethics
- Encryption
- Master decrypt key
- Terms of Service
- Data Location
- Exit Strategy
- “Zero knowledge”

# Cloud Services

- Dropbox
- OneDrive
- iCloud
- Google Drive
- Box
- Citrix ShareFile
- SpiderOak
- Boxcryptor/Sookasa/Viivo & other bolt-ons



# Legal Cloud Computing Assn.

- Released security standards for cloud computing by lawyers on March 17, 2016
- Restrict where data is located
- Certifications
- Multiple locations of data
- Encryption
- Pen testing and vulnerability scans
- Access control by 3<sup>rd</sup> parties
- Data destruction and retention policies
- Disaster recovery



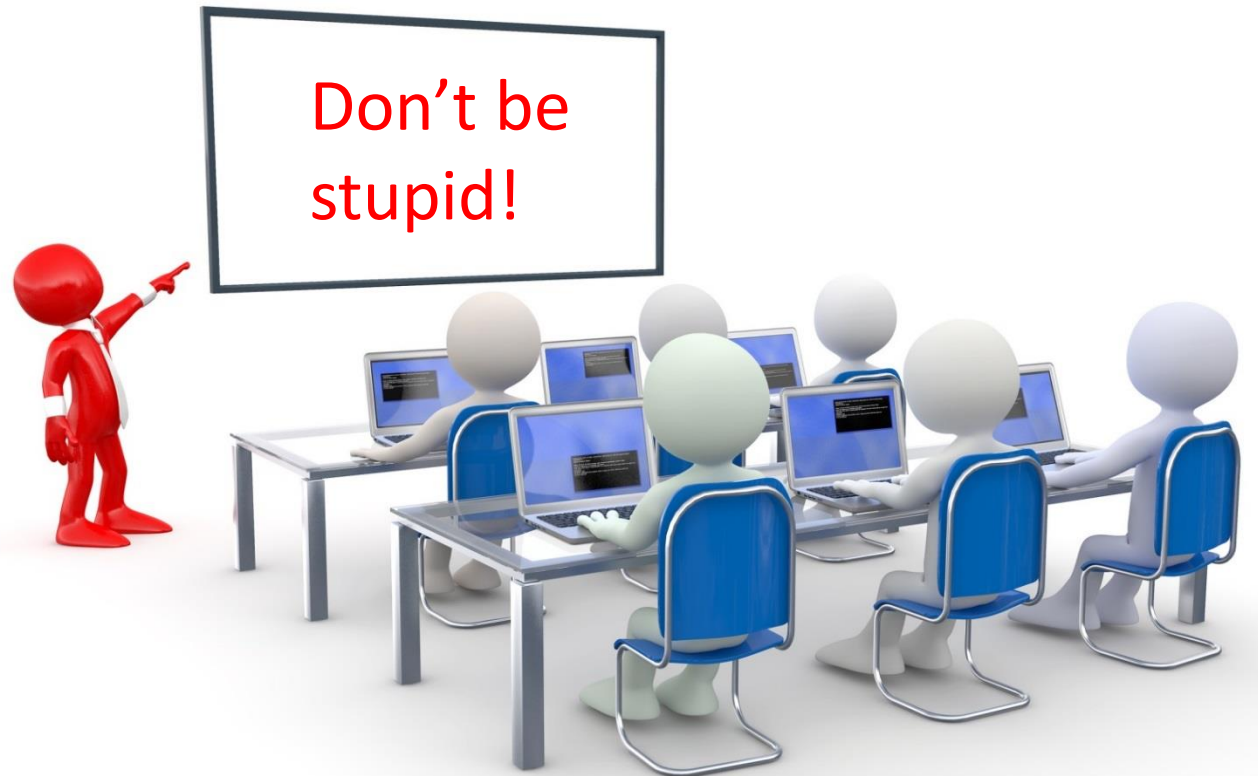



# Legal Cloud Computing Assn.

- User authentication
- Adding/suspending users
- Audit logs
- User ability to add/delete data
- Retrieval of data in usable format
- Terms of Service
- Privacy policy
- Update guarantee
- Confidentiality
- Ownership
- Demands for data
- Data breaches



# Training Training Training Have We Mentioned Training?





Allways chek for  
speling erors

# Training

- Phishing, especially spear phishing – most successful way of breaching law firms
- CEO scams – FBI alert, 2.3 billion, 270% increase Jan. 2015-Feb. 2016
- Drive-by infections
- Sharing credentials
- Piggybacking
- Social engineering
- Every year







*"The user's going to pick dancing pigs over security every time."*

*Bruce Schneier*

# Social media – users ignore policies and training







# Public computers – never use for work



# Secure remote access

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



# Wireless Networks

- Default values – change the defaults!
- Drive-by
- Used by spammers
- Used by neighbors to ride your access, download porn, etc.



# Wireless



- WiFi
  - Hotspots
  - ~~WEP~~
  - ~~WPA~~
  - WPA2
- MiFi
  - Tethering
- How do you connect safely? VPN – or bring up a hotspot on your phone

# 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. Blackphone and “the Black”
2. Android
3. iPhone
4. BlackBerry
5. Windows 10  
Symbian  
WebOS

# Cell phone anti-malware (iPhone and Android)

- Sophos
- Lookout
- Kaspersky
- McAfee
- Can't protect iPhone's kernel



# 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



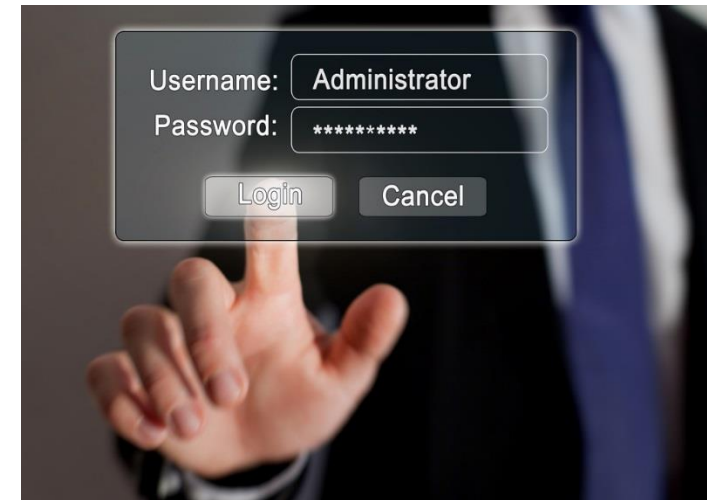
# Physical Security

- Servers belong in a locked room
- Biometric access to the room
- Recording cameras and motion sensors
- Locked fire safes for backup media and locked server cabinets or racks



# Access Control

- Does a secretary need access to financial records?
- Access control is usually inadequate
- Access control frequently goes unreviewed – must be done regularly
- Who monitors the person who sets the access?
- Is everything logged?



# The Need for Background Checks

- Kevin Mitnick – a law firm systems admin?
- They dodged a bullet

Then



Now



# What are we outsourcing?

## Duty to supervise and ensure security!

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



**DANCE LIKE NO ONE'S WATCHING.  
ENCRYPT LIKE EVERYONE IS!**



