FARHANG & MEDCOFF
Attorneys
FULL SERVICE LAW FIRM

Best Lawyers
BEST
LAW FIRMS
U.S.News
2018

www.fmlaw.law

esi
evidence solutions, inc.

Farhang & Medcoff,
Evidence Solutions, Inc.
And the
Arizona Technology Council

Present:

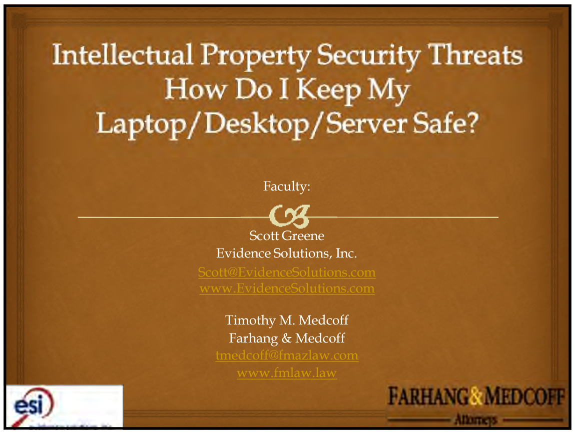
Prevent IP Theft:
Protect Your Most Valuable Assets from Employee and Vendor Theft

January 24, 2018
Courtyard Marriott
201 S Williams Blvd
Tucson, AZ 85711, USA

Presented by:

Scott Greene, SCFE, CEO
Evidence Solutions, Inc.

Tim Medcoff, Managing Partner
Farhang & Medcoff



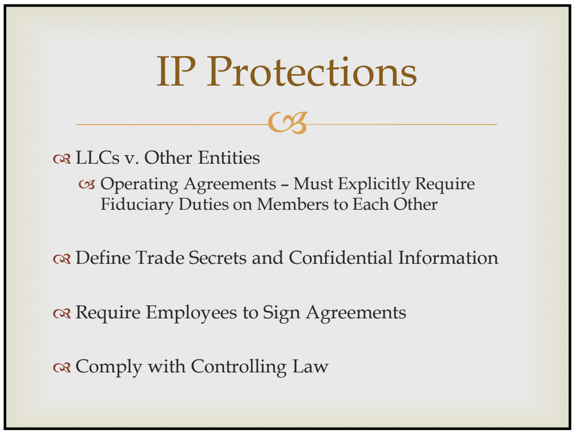
Intellectual Property Security Threats How Do I Keep My Laptop/Desktop/Server Safe?

Faculty:

Scott Greene
Evidence Solutions, Inc.
Scott@EvidenceSolutions.com
www.EvidenceSolutions.com

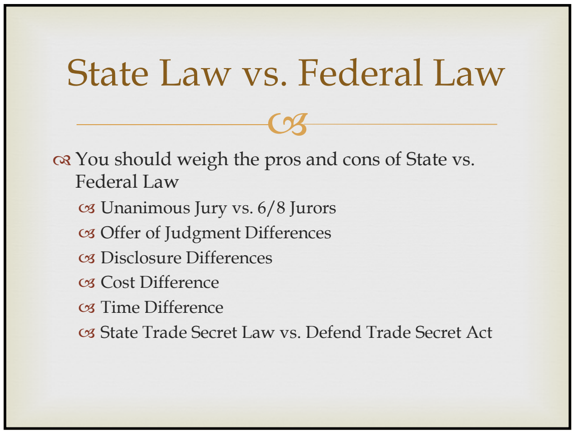
Timothy M. Medcoff
Farhang & Medcoff
tmedcoff@fmazlaw.com
www.fmlaw.law

FARHANG&MEDCOFF
Attorneys



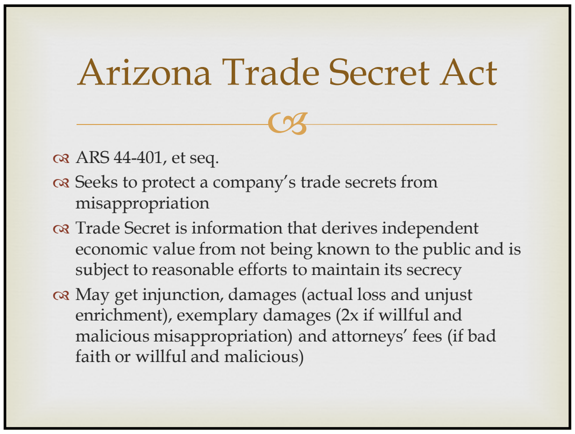
IP Protections

- LLCs v. Other Entities
  - Operating Agreements – Must Explicitly Require Fiduciary Duties on Members to Each Other
- Define Trade Secrets and Confidential Information
- Require Employees to Sign Agreements
- Comply with Controlling Law



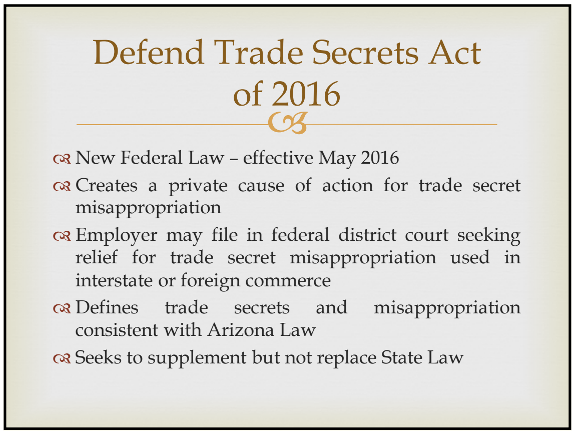
State Law vs. Federal Law

- You should weigh the pros and cons of State vs. Federal Law
  - Unanimous Jury vs. 6/8 Jurors
  - Offer of Judgment Differences
  - Disclosure Differences
  - Cost Difference
  - Time Difference
  - State Trade Secret Law vs. Defend Trade Secret Act



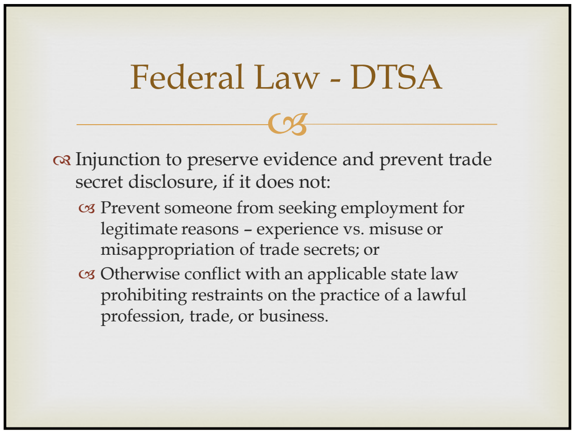
Arizona Trade Secret Act

- ARS 44-401, et seq.
- Seeks to protect a company's trade secrets from misappropriation
- Trade Secret is information that derives independent economic value from not being known to the public and is subject to reasonable efforts to maintain its secrecy
- May get injunction, damages (actual loss and unjust enrichment), exemplary damages (2x if willful and malicious misappropriation) and attorneys' fees (if bad faith or willful and malicious)



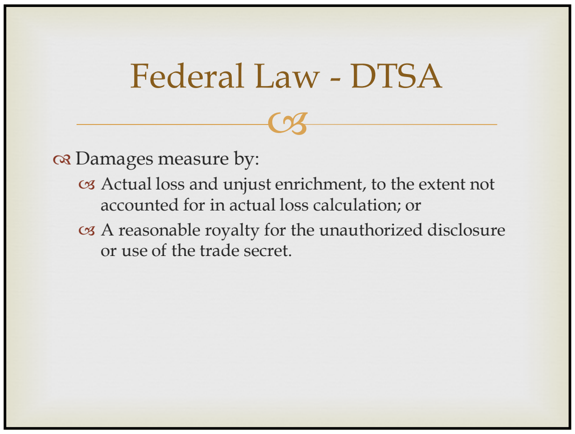
Defend Trade Secrets Act of 2016

- New Federal Law – effective May 2016
- Creates a private cause of action for trade secret misappropriation
- Employer may file in federal district court seeking relief for trade secret misappropriation used in interstate or foreign commerce
- Defines trade secrets and misappropriation consistent with Arizona Law
- Seeks to supplement but not replace State Law



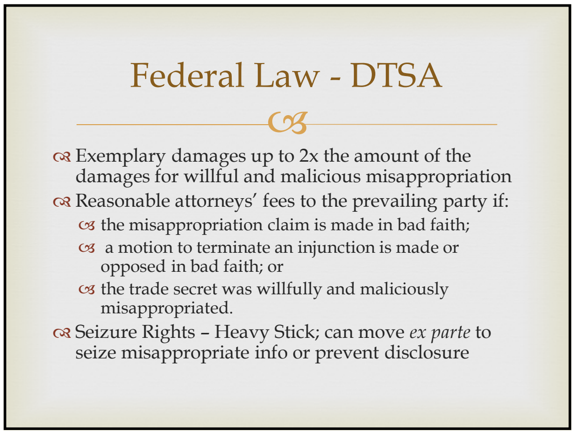
Federal Law - DTSA

- Injunction to preserve evidence and prevent trade secret disclosure, if it does not:
  - Prevent someone from seeking employment for legitimate reasons – experience vs. misuse or misappropriation of trade secrets; or
  - Otherwise conflict with an applicable state law prohibiting restraints on the practice of a lawful profession, trade, or business.



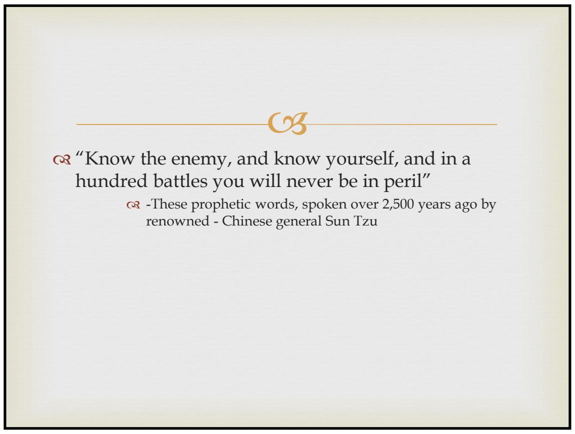
Federal Law - DTSA

- Damages measure by:
  - Actual loss and unjust enrichment, to the extent not accounted for in actual loss calculation; or
  - A reasonable royalty for the unauthorized disclosure or use of the trade secret.

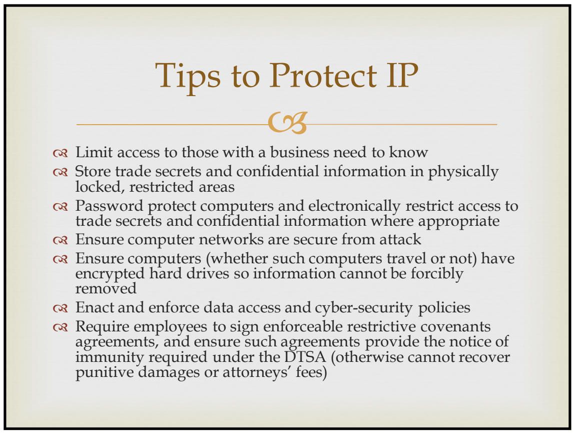


Federal Law - DTSA

- Exemplary damages up to 2x the amount of the damages for willful and malicious misappropriation
- Reasonable attorneys' fees to the prevailing party if:
  - the misappropriation claim is made in bad faith;
  - a motion to terminate an injunction is made or opposed in bad faith; or
  - the trade secret was willfully and maliciously misappropriated.
- Seizure Rights – Heavy Stick; can move *ex parte* to seize misappropriate info or prevent disclosure



- “Know the enemy, and know yourself, and in a hundred battles you will never be in peril”
  - -These prophetic words, spoken over 2,500 years ago by renowned - Chinese general Sun Tzu

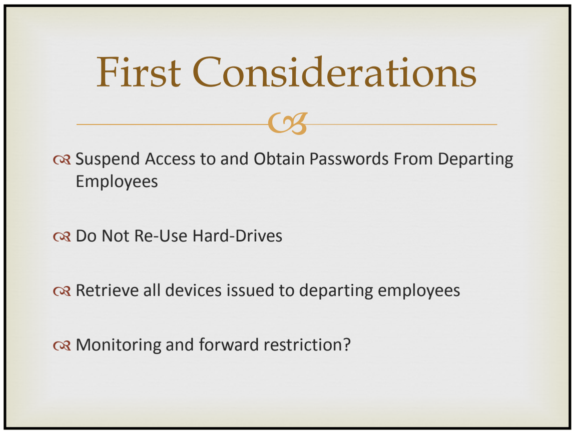


Tips to Protect IP

- Limit access to those with a business need to know
- Store trade secrets and confidential information in physically locked, restricted areas
- Password protect computers and electronically restrict access to trade secrets and confidential information where appropriate
- Ensure computer networks are secure from attack
- Ensure computers (whether such computers travel or not) have encrypted hard drives so information cannot be forcibly removed
- Enact and enforce data access and cyber-security policies
- Require employees to sign enforceable restrictive covenants agreements, and ensure such agreements provide the notice of immunity required under the DTSA (otherwise cannot recover punitive damages or attorneys’ fees)

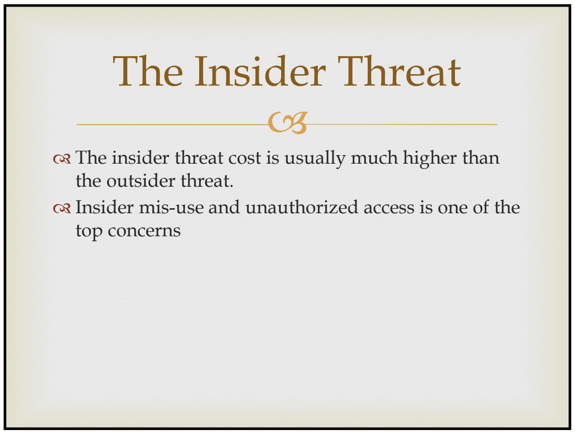
First Considerations

- Take the steps Necessary to Protect and Organize Your Data Before You Have a Problem
- Identify and safeguard access to trade secrets and confidential information to the extent possible.
- Implement appropriate Policies and Notifications to Employees



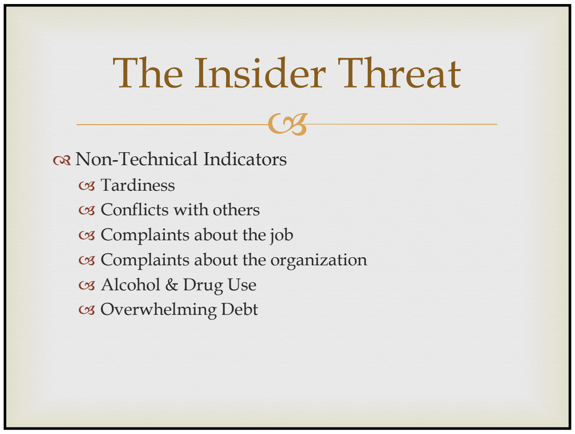
First Considerations

- Suspend Access to and Obtain Passwords From Departing Employees
- Do Not Re-Use Hard-Drives
- Retrieve all devices issued to departing employees
- Monitoring and forward restriction?



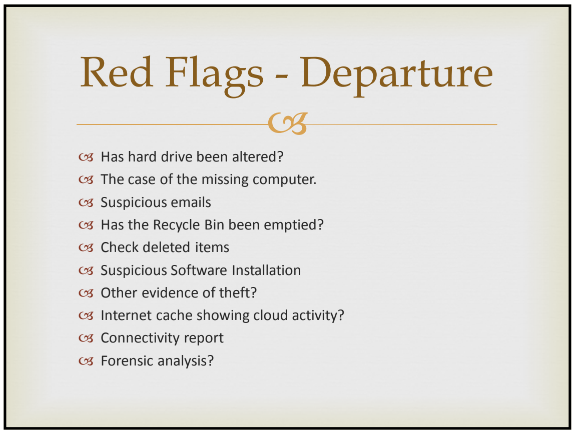
The Insider Threat

- The insider threat cost is usually much higher than the outsider threat.
- Insider mis-use and unauthorized access is one of the top concerns



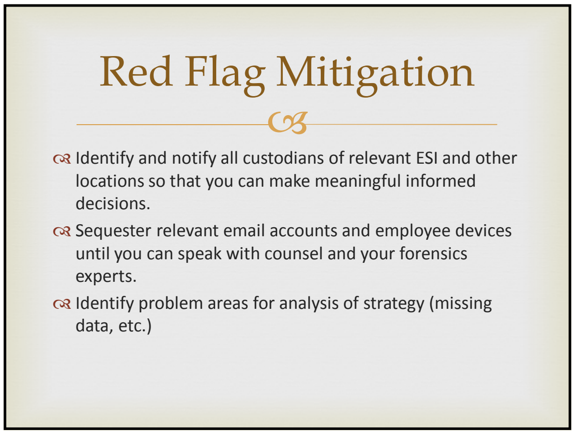
The Insider Threat

- Non-Technical Indicators
  - Tardiness
  - Conflicts with others
  - Complaints about the job
  - Complaints about the organization
  - Alcohol & Drug Use
  - Overwhelming Debt



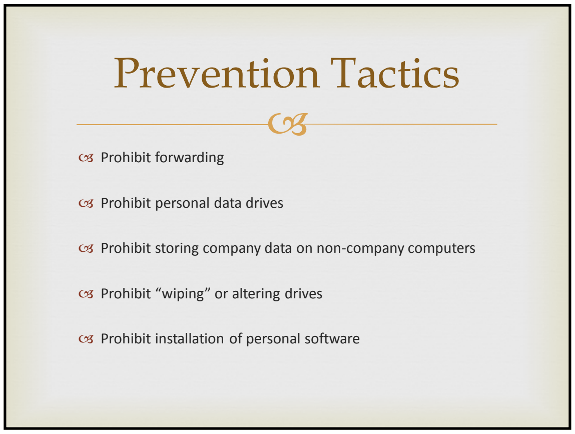
Red Flags - Departure

- Has hard drive been altered?
- The case of the missing computer.
- Suspicious emails
- Has the Recycle Bin been emptied?
- Check deleted items
- Suspicious Software Installation
- Other evidence of theft?
- Internet cache showing cloud activity?
- Connectivity report
- Forensic analysis?



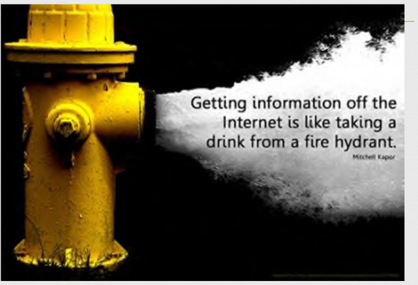
Red Flag Mitigation

- Identify and notify all custodians of relevant ESI and other locations so that you can make meaningful informed decisions.
- Sequester relevant email accounts and employee devices until you can speak with counsel and your forensics experts.
- Identify problem areas for analysis of strategy (missing data, etc.)



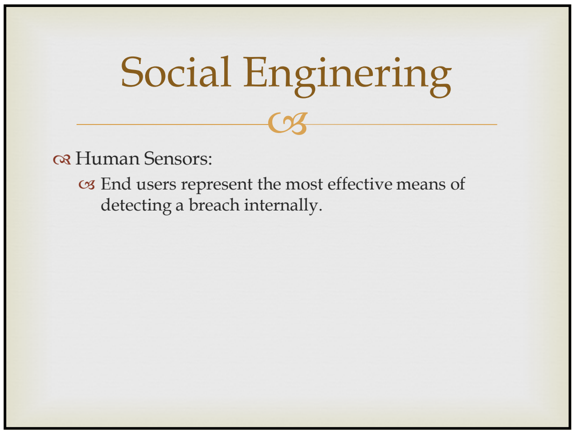
Prevention Tactics

- Prohibit forwarding
- Prohibit personal data drives
- Prohibit storing company data on non-company computers
- Prohibit “wiping” or altering drives
- Prohibit installation of personal software


Getting information off the Internet is like taking a drink from a fire hydrant.
Mitchell Kapor

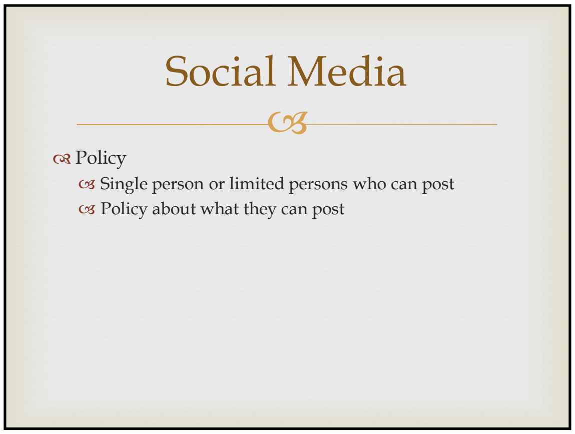
People People People

- Organizations with educated users have fewer problems.
  - Threats to organizations
    - Social engineering
    - Sloppy users
      - End users are fooled into opening attachments and loading software from untrusted sites, visiting web sites where they are infected and more.
      - System administrators are also fooled like normal users but are also tested when:
        - unauthorized accounts are set up on their systems, when unauthorized equipment is attached, when large amounts of data are exfiltrated.



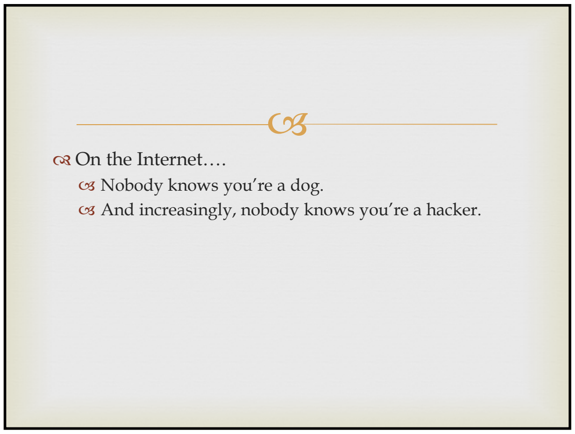
Social Enginering

- Human Sensors:
  - End users represent the most effective means of detecting a breach internally.

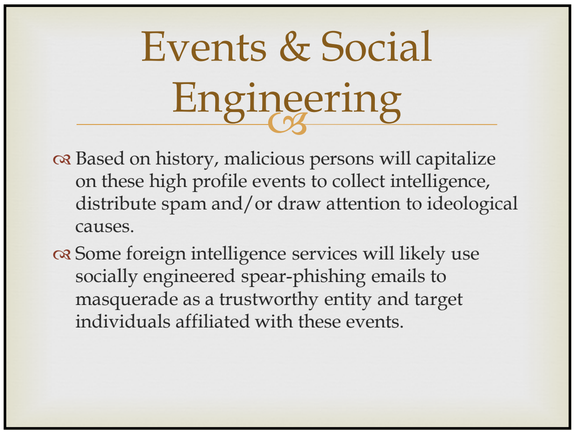


Social Media

- Policy
  - Single person or limited persons who can post
  - Policy about what they can post

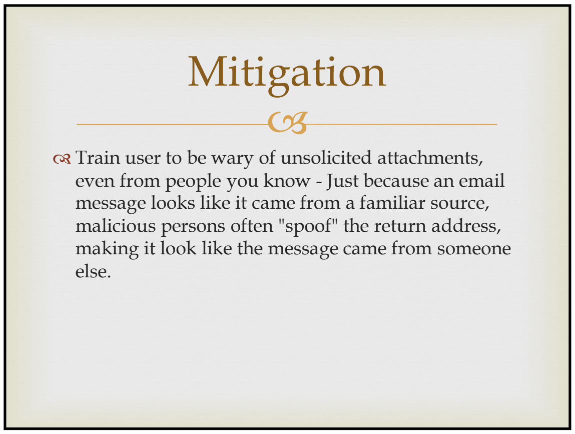


- On the Internet….
  - Nobody knows you're a dog.
  - And increasingly, nobody knows you're a hacker.



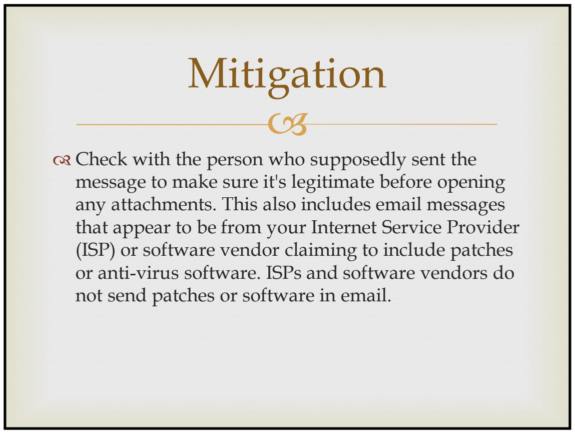
Events & Social Engineering

- Based on history, malicious persons will capitalize on these high profile events to collect intelligence, distribute spam and/or draw attention to ideological causes.
- Some foreign intelligence services will likely use socially engineered spear-phishing emails to masquerade as a trustworthy entity and target individuals affiliated with these events.



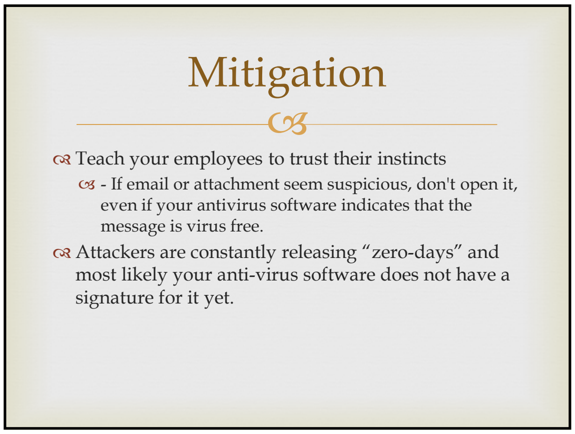
Mitigation

- Train user to be wary of unsolicited attachments, even from people you know - Just because an email message looks like it came from a familiar source, malicious persons often "spoof" the return address, making it look like the message came from someone else.



Mitigation

- Check with the person who supposedly sent the message to make sure it's legitimate before opening any attachments. This also includes email messages that appear to be from your Internet Service Provider (ISP) or software vendor claiming to include patches or anti-virus software. ISPs and software vendors do not send patches or software in email.

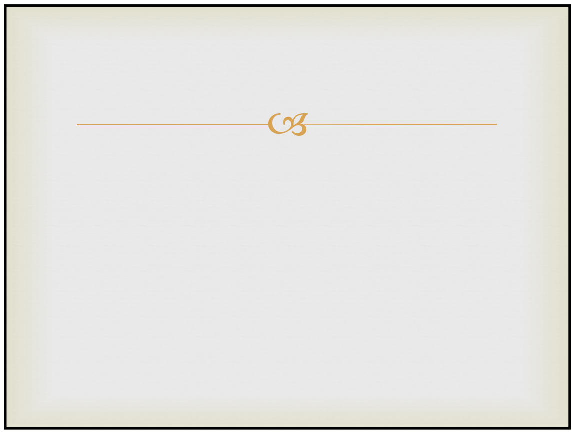


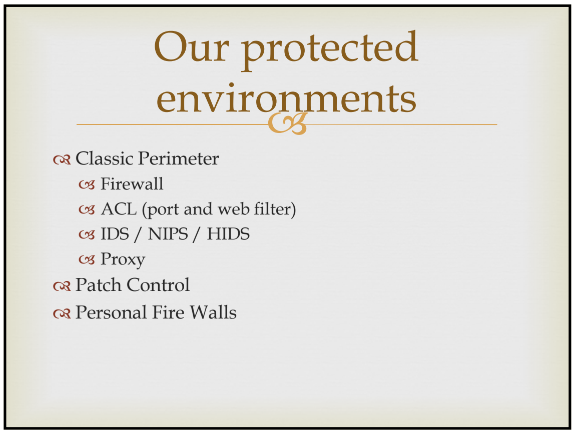
Mitigation

- Teach your employees to trust their instincts
  - - If email or attachment seem suspicious, don't open it, even if your antivirus software indicates that the message is virus free.
- Attackers are constantly releasing "zero-days" and most likely your anti-virus software does not have a signature for it yet.

Mitigation

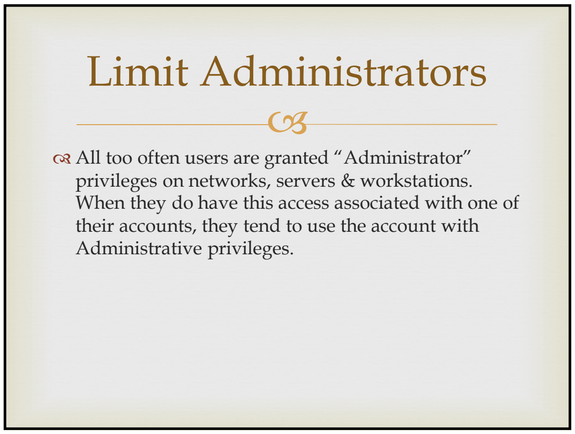
- Personal Firewalls
  - Zone Alarm
  - Comodo
  - Norton Internet Security
  - Bit Defender
  - McAfee Internet Security





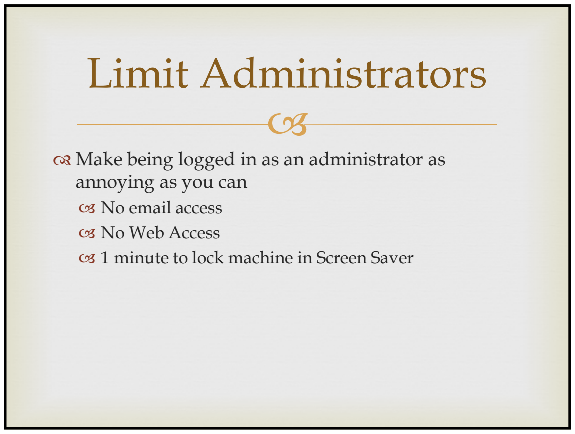
Our protected environments

- Classic Perimeter
  - Firewall
  - ACL (port and web filter)
  - IDS / NIPS / HIDS
  - Proxy
- Patch Control
- Personal Fire Walls



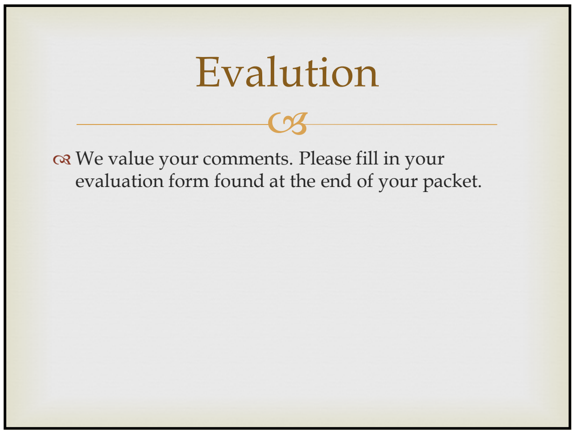
Limit Administrators

- All too often users are granted "Administrator" privileges on networks, servers & workstations. When they do have this access associated with one of their accounts, they tend to use the account with Administrative privileges.



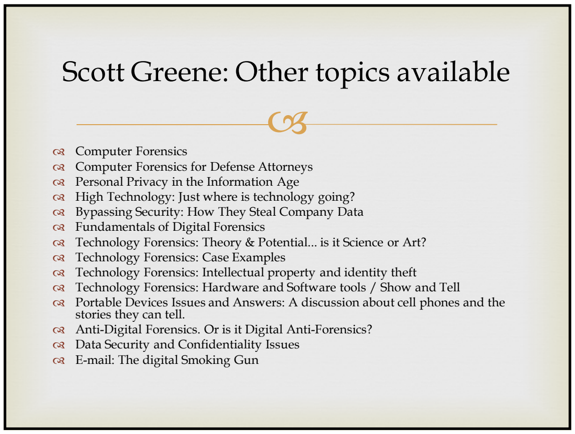
Limit Administrators

- Make being logged in as an administrator as annoying as you can
  - No email access
  - No Web Access
  - 1 minute to lock machine in Screen Saver



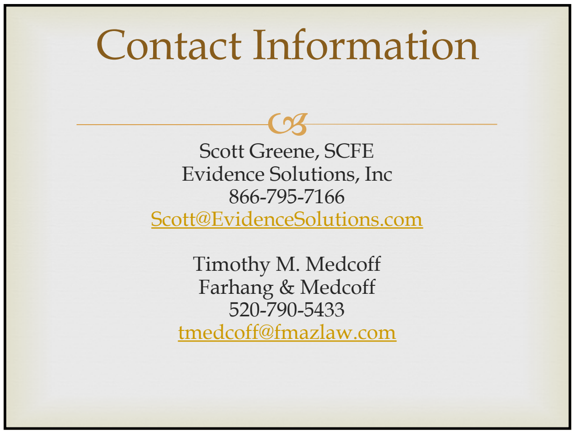
Evalution

- We value your comments. Please fill in your evaluation form found at the end of your packet.



Scott Greene: Other topics available

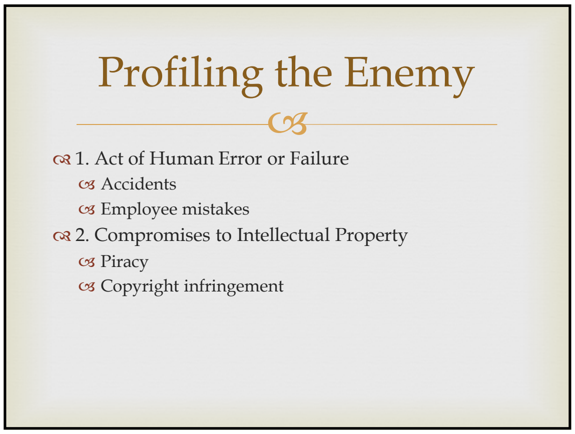
- Computer Forensics
- Computer Forensics for Defense Attorneys
- Personal Privacy in the Information Age
- High Technology: Just where is technology going?
- Bypassing Security: How They Steal Company Data
- Fundamentals of Digital Forensics
- Technology Forensics: Theory & Potential… is it Science or Art?
- Technology Forensics: Case Examples
- Technology Forensics: Intellectual property and identity theft
- Technology Forensics: Hardware and Software tools / Show and Tell
- Portable Devices Issues and Answers: A discussion about cell phones and the stories they can tell.
- Anti-Digital Forensics. Or is it Digital Anti-Forensics?
- Data Security and Confidentiality Issues
- E-mail: The digital Smoking Gun



Contact Information

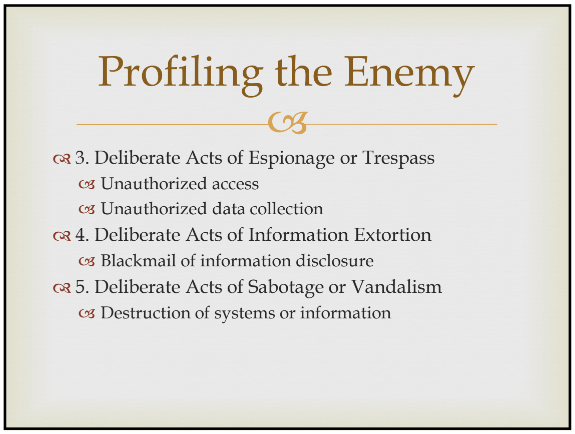
Scott Greene, SCFE
Evidence Solutions, Inc
866-795-7166
Scott@EvidenceSolutions.com

Timothy M. Medcoff
Farhang & Medcoff
520-790-5433
tmedcoff@fmazlaw.com



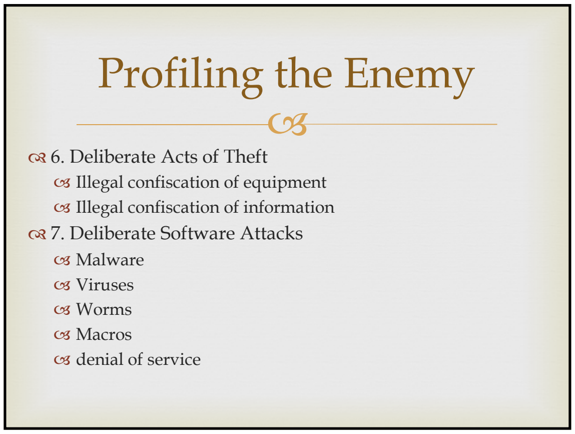
Profiling the Enemy

- 1. Act of Human Error or Failure
  - Accidents
  - Employee mistakes
- 2. Compromises to Intellectual Property
  - Piracy
  - Copyright infringement



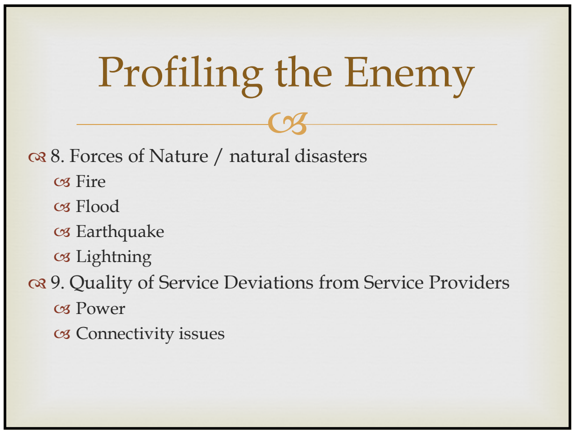
Profiling the Enemy

- 3. Deliberate Acts of Espionage or Trespass
  - Unauthorized access
  - Unauthorized data collection
- 4. Deliberate Acts of Information Extortion
  - Blackmail of information disclosure
- 5. Deliberate Acts of Sabotage or Vandalism
  - Destruction of systems or information



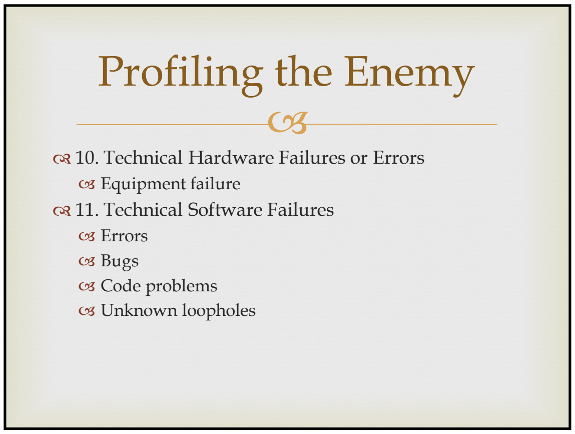
Profiling the Enemy

- 6. Deliberate Acts of Theft
  - Illegal confiscation of equipment
  - Illegal confiscation of information
- 7. Deliberate Software Attacks
  - Malware
  - Viruses
  - Worms
  - Macros
  - denial of service



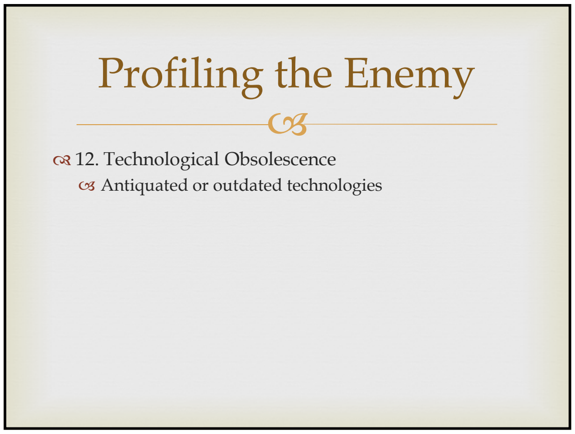
Profiling the Enemy

- 8. Forces of Nature / natural disasters
  - Fire
  - Flood
  - Earthquake
  - Lightning
- 9. Quality of Service Deviations from Service Providers
  - Power
  - Connectivity issues



Profiling the Enemy

- 10. Technical Hardware Failures or Errors
  - Equipment failure
- 11. Technical Software Failures
  - Errors
  - Bugs
  - Code problems
  - Unknown loopholes



Profiling the Enemy

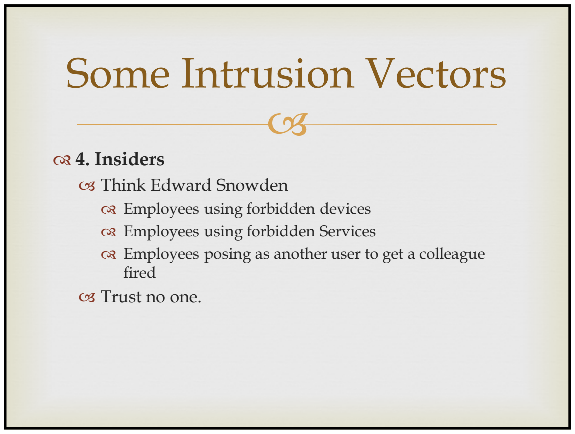
- 12. Technological Obsolescence
  - Antiquated or outdated technologies

Famous Hacking Events

- U.S. Weapons Systems
  - Author: Suspected Chinese (Unofficial)
  - Target: Weapons Systems Design

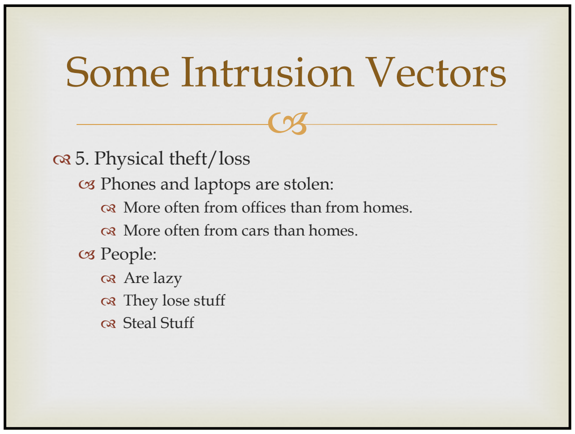
Some Intrusion Vectors

- **1. Web app attacks**
  - This is the most common type of data breach.
  - Primarily accomplished via Phishing / Spear Phishing
  - Then malware is installed.
  - Then they correctly guess your pet's name, your son's name and your nickname.
  - Prevention: Two Factor Authentication



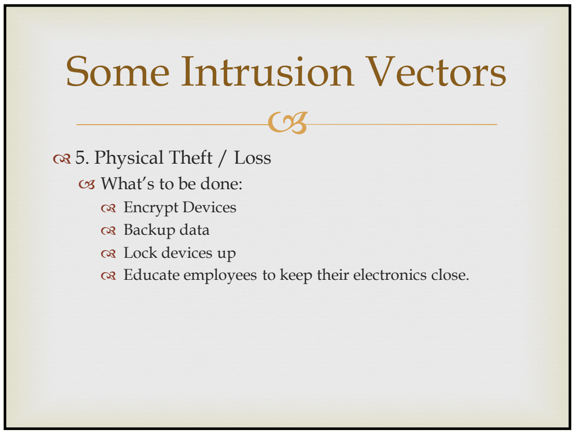
Some Intrusion Vectors

- **4. Insiders**
  - Think Edward Snowden
    - Employees using forbidden devices
    - Employees using forbidden Services
    - Employees posing as another user to get a colleague fired
  - Trust no one.



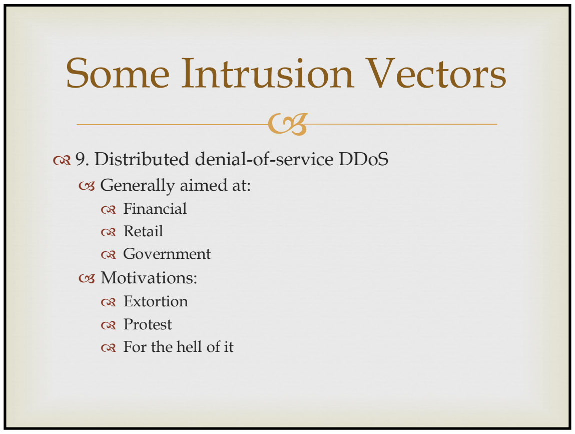
Some Intrusion Vectors

- 5. Physical theft/loss
  - Phones and laptops are stolen:
    - More often from offices than from homes.
    - More often from cars than homes.
  - People:
    - Are lazy
    - They lose stuff
    - Steal Stuff



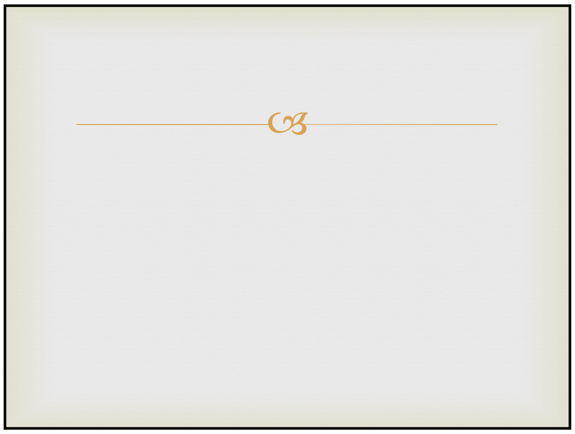
Some Intrusion Vectors

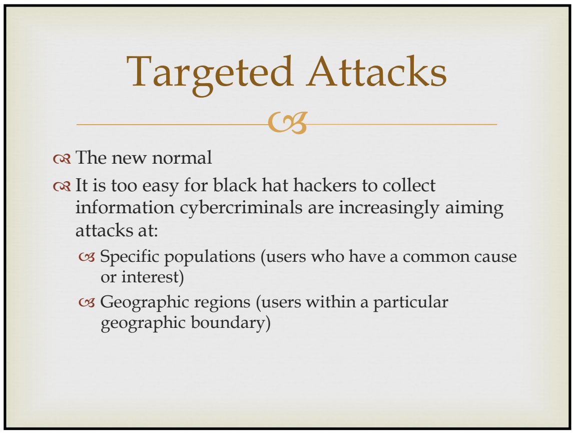
- 5. Physical Theft / Loss
  - What's to be done:
    - Encrypt Devices
    - Backup data
    - Lock devices up
    - Educate employees to keep their electronics close.



Some Intrusion Vectors

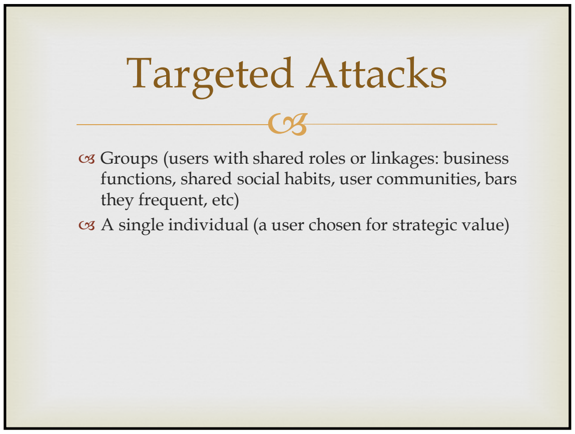
- 9. Distributed denial-of-service DDoS
  - Generally aimed at:
    - Financial
    - Retail
    - Government
  - Motivations:
    - Extortion
    - Protest
    - For the hell of it





Targeted Attacks

- The new normal
- It is too easy for black hat hackers to collect information cybercriminals are increasingly aiming attacks at:
  - Specific populations (users who have a common cause or interest)
  - Geographic regions (users within a particular geographic boundary)



Targeted Attacks

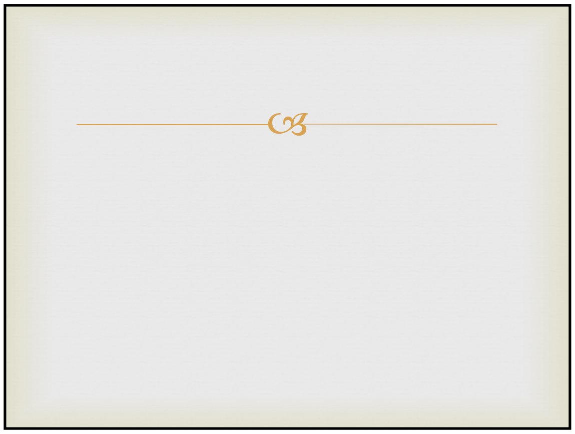
- Groups (users with shared roles or linkages: business functions, shared social habits, user communities, bars they frequent, etc)
- A single individual (a user chosen for strategic value)

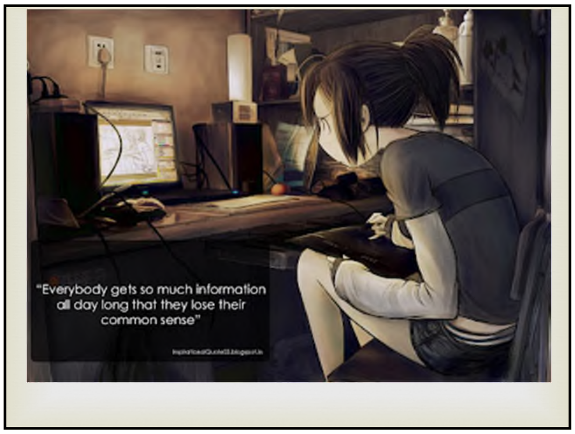
The Cost to Organizations

- A Juniper Research report indicates there will be 16,000 data breaches which will cost over $2 Trillian

Famous Hacking Events

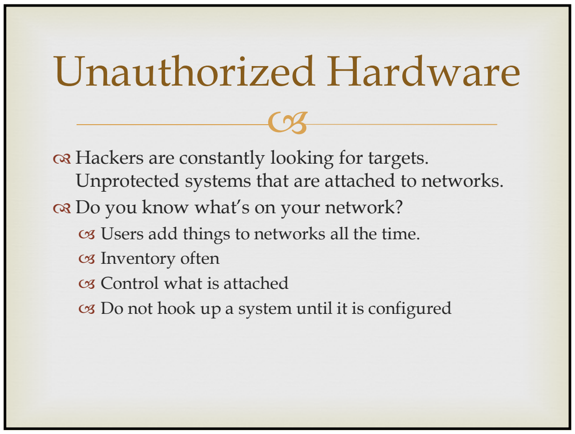
- Hacking Team
- It sells its products to the US Federal Government and other Governments





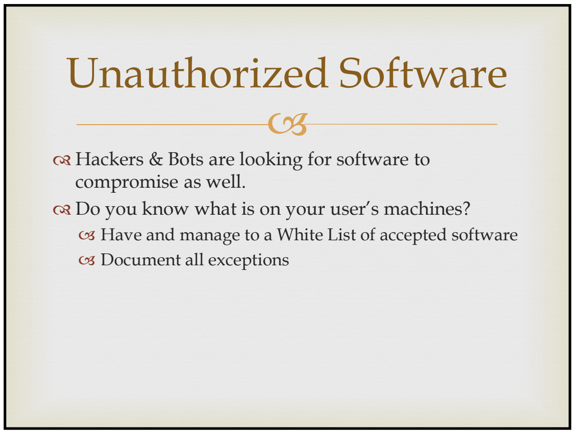
"Everybody gets so much information all day long that they lose their common sense"

InspirationalQuote33.blogspot.in



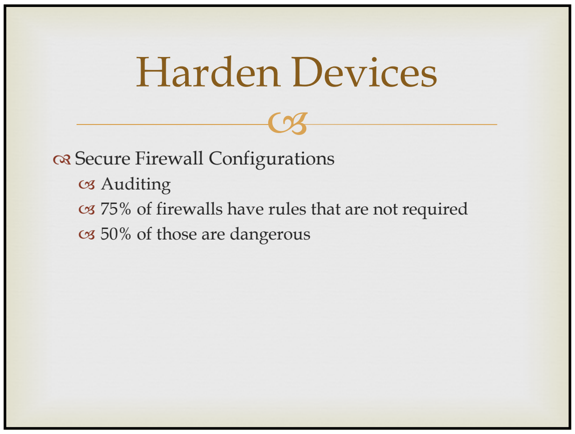
Unauthorized Hardware

- Hackers are constantly looking for targets. Unprotected systems that are attached to networks.
- Do you know what's on your network?
  - Users add things to networks all the time.
  - Inventory often
  - Control what is attached
  - Do not hook up a system until it is configured



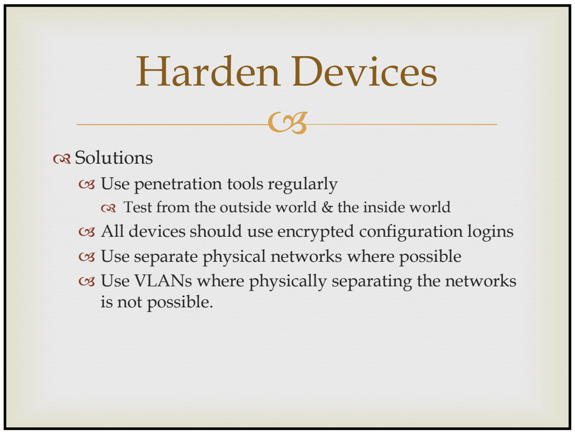
Unauthorized Software

- Hackers & Bots are looking for software to compromise as well.
- Do you know what is on your user's machines?
  - Have and manage to a White List of accepted software
  - Document all exceptions



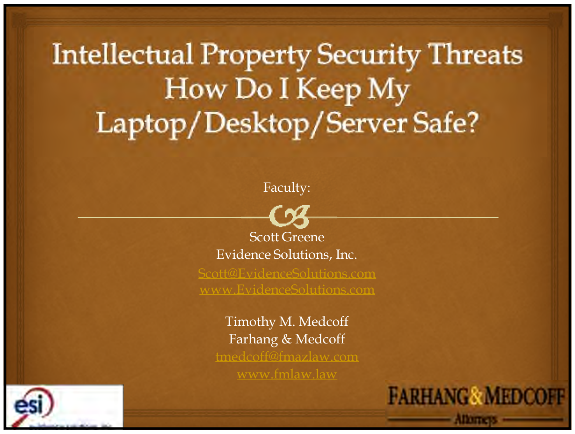
Harden Devices

- Secure Firewall Configurations
  - Auditing
  - 75% of firewalls have rules that are not required
  - 50% of those are dangerous



Harden Devices

- Solutions
  - Use penetration tools regularly
    - Test from the outside world & the inside world
  - All devices should use encrypted configuration logins
  - Use separate physical networks where possible
  - Use VLANs where physically separating the networks is not possible.



Intellectual Property Security Threats How Do I Keep My Laptop/Desktop/Server Safe?

Faculty:

Scott Greene
Evidence Solutions, Inc.
Scott@EvidenceSolutions.com
www.EvidenceSolutions.com

Timothy M. Medcoff
Farhang & Medcoff
tmedcoff@fmazlaw.com
www.fmlaw.law

esi
FARHANG&MEDCOFF
Attorneys

esi
evidence solutions, inc.

Seminar Evaluation Form

Date: _____ ____________________

	Poor	Ok	Good	Very Good	Excellent
1. Was the material informative?	**1**	**2**	**3**	**4**	**5**
2. Was the material easy to understand?	**1**	**2**	**3**	**4**	**5**
3. Was the material appropriate?	**1**	**2**	**3**	**4**	**5**
4. Was the material interesting?	**1**	**2**	**3**	**4**	**5**
5. Was the medium used to present this subject effective?	**1**	**2**	**3**	**4**	**5**
6. The material presented in the seminar will be of use to me.	**1**	**2**	**3**	**4**	**5**
7. The material presented was properly sequenced.	**1**	**2**	**3**	**4**	**5**
8. Was the speaker effective?	**1**	**2**	**3**	**4**	**5**
9. The seminar was well worth my time.	**1**	**2**	**3**	**4**	**5**

10. Have you relied on computer forensics in your previous experience? **YES** _____ **NO** _____

12. General impression of material presented? ____

____

____

13. Why did you attend this seminar today? ____

____

____

14. Would you like someone to contact you about computer forensics? **YES** ______ **NO** ______

Name: ____

Address: ____

Mailing Address: ____
(if different)

Email: ____

Phone: (   ) ______________________ **Fax:** (   ) ______________________

Comments may be used on EvidenceSolutions.com. Please let me know if you object.