SHIELDING YOUR FIRM: Identifying Threats & Protecting Your Sensitive Data

Faculty: Scott Greene of Evidence Solutions, Inc.

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

Pop Quiz

- Who is the enemy?
- What do you believe the solutions are?

PROFILING THE ENEMY

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

PROFILING THE ENEMY

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

PROFILING THE ENEMY

- Deliberate Acts of Theft
  - Illegal confiscation of equipment
  - Illegal confiscation of information
- Deliberate Software Attacks
  - Malware
  - Viruses
  - Worms
  - Macros
  - Denial of service

PROFILING THE ENEMY

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

PROFILING THE ENEMY

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

PROFILING THE ENEMY

- Technological Obsolescence
  - Antiquated or outdated technologies

THE COST TO ORGANIZATIONS

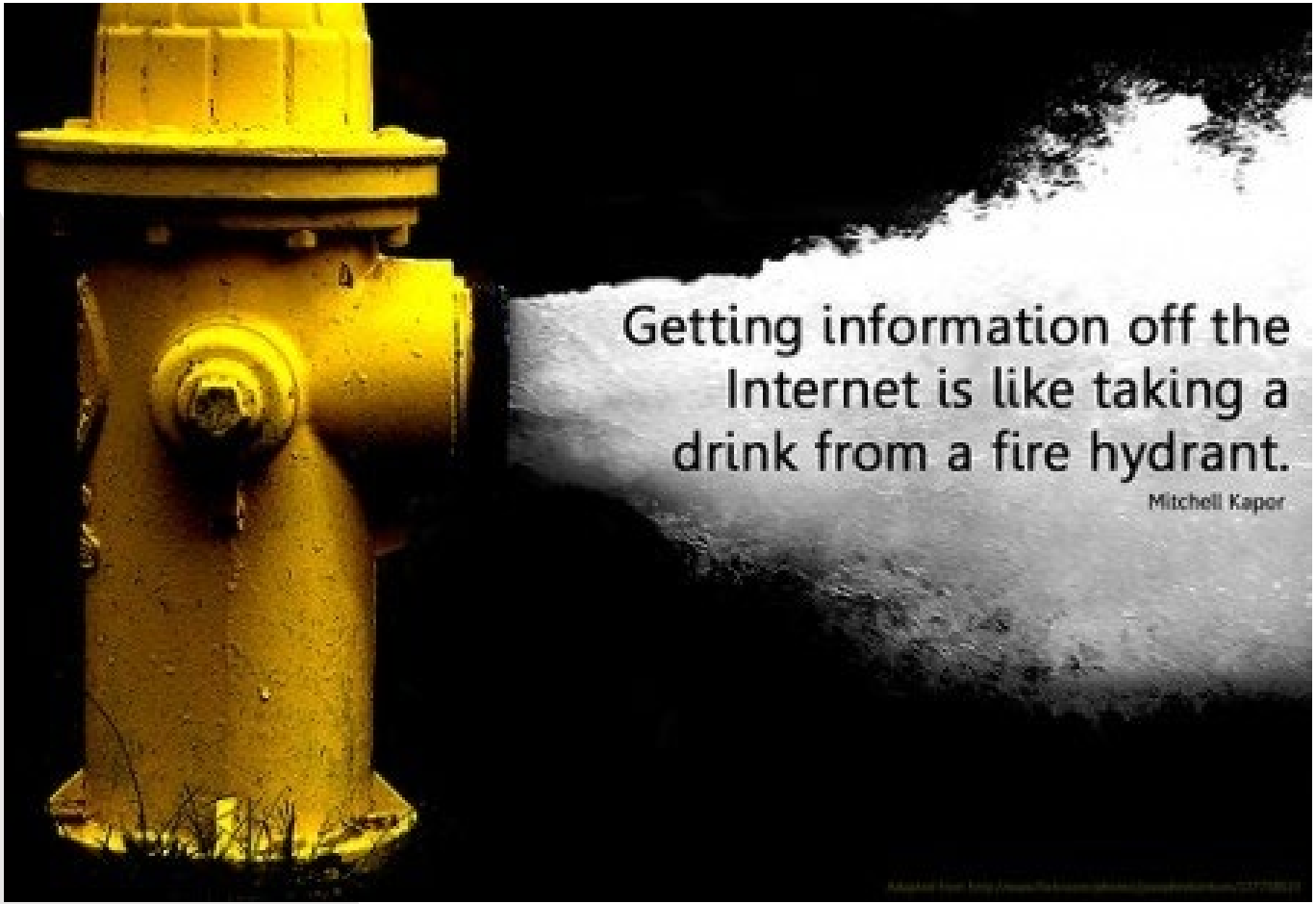
- A Juniper Research report indicates there will be 16,000 data breaches which will cost over $2 Trillian

SOME INTRUSION VECTORS

- 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

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


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

MALWARE | RANSOMWARE

- 70,000 new malware strains are detected every day.
- Patches eliminate most of them.
- Training employees to not open attached eliminates most of the rest.

MALWARE | RANSOMWARE

- Law Firms are Particularly Good Targets
  - Sensitive Client Data
  - Requirement of Confidentiality
  - Threat Actors leverage legal and ethical obligations to force ransom payments.

MALWARE | RANSOMWARE

- After an Attack
  - Nearly 70% of Law Firms attacked paid ransoms to regain access / retrieve stolen data.
  - Risk of being double crossed is high.
    - 1/3 of those who complied never recovered their files.

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

PEOPLE PEOPLE PEOPLE

- Organizations with educated users have fewer problems.

PEOPLE PEOPLE PEOPLE

- 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 ENGINEERING

- 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.

THE INSIDER THREAT

- The insider threat cost is usually much higher than the outsider threat.
  - Opening attachments when they shouldn't!
  - 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

EVENTS & SOCIAL ENGINEERING

- Based on history, malicious persons will capitalize on these 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.

CASE EXAMPLES

I regularly investigate Social Engineering Cases…

CASE EXAMPLES

- National Real Estate firm:
  - The Title and Escrow company was mimicked by the bad actor.
  - They created a domain just 1 character off the real domain
  - The bad actor managed to get $180k wired to the wrong account and they were gone!

CASE EXAMPLES

- A Contracting Firm was relieved of $185,000 when they interacted with a firm they thought was a sub-contractor.
  - The bad actor created… a domain with one extra character in the domain name.
  - They interacted with the victim firm and managed to get someone in the AP department to wire data to the bad actor.

CASE EXAMPLES

- A Canadian Law Firm

Silly Things To Do & Not To Do

SILLY THINGS TO DO & NOT TO DO

- Use a password manager!!!
  - Dashlane
  - 1Password
  - LastPass
  - Zoho Vault

SILLY THINGS TO DO & NOT TO DO

- Connect to networks you shouldn't connect to:
  - Rental Cars - Noooooooooooo
  - Connecting your cell phone to a car can leave behind contacts, text message, email and more!

SILLY THINGS TO DO & NOT TO DO

- Physical Security
  - Hotels:
  - Do Not Disturb on the door
  - Call the front Desk
  - Use a Safe
  - Or
  - Use a Laptop lock

SILLY THINGS TO DO & NOT TO DO

- Physical Security
  - Watch your stuff at ALL TSA check points!
    - I personally know two people who have lost laptops at check points.
    - Last week I watched a lady walk off w/o hers. I managed to get her to come back and she was re-united with her machine.
  - Do not leave laptops or other important stuff in the car where it is visible!
    - Stuff can disappear in seconds.

SILLY THINGS TO DO & NOT TO DO

- Two Factor Authentication!
  - Aka 2FA
  - Requires 2 different ways to identify yourself to a system.
- Virtual Private Networks
  - When you are traveling
  - From Airports & From Hotels
  - From Opposing Counsel offices…

SILLY THINGS TO DO & NOT TO DO

- Internet of Things aka IOT
  - Don’t, just Don’t
  - Alexa listens all the time
  - Siri listens all the time
  - Google Assistant listens all the time
  - Don’t buy devices, appliances, etc. that require being connected to the internet.

RESOURCES

- National Institute of Standards & Technology
  - Nist.gov
  - NIST has popularized the “Phish Scale” as a method to better characterize an organization’s phishing risk.
    - How this ranking is done is available on the NIST Site.
  - https://www.nist.gov/cybersecurity/cybersecurity-privacy-stakeholder-engagement

RESOURCES

- National White Collar Crime Center:
  - https://www.nw3c.org/online-training
- ESET
  - https://www.eset.com/us/cybertraining/
- SANS
  - https://www.sans.org/security-awareness-training/products/security-awareness-solutions/end-user/
- Others:
  - https://www.comparitech.com/blog/information-security/best-cyber-security-awareness-courses/
- Free!
- Encourage employees to watch one per week and report what they learned.
- Encourage clients to watch one per week.

RESOURCES

Subscribe to the Evidence Solutions Newsletter!

- www.EvidenceSolutions.com

Contact Information

Scott Greene, SCFE
Evidence Solutions, Inc.
866.795.7166
Scott@EvidenceSolutions.com