Evidence Solutions, Inc.

&

Leading Age

Present:

Protecting Electronic Medical Record Systems - Digital Information Security For Health Care Providers

Tuesday, September15, 2015

2:00 PM – 4:00 PM

Presented by:

Scott Greene, SCFE, CEO
Evidence Solutions, Inc

Computer Forensics
Cell Phone Forensics
Electronic Medical Record Forensics

866-795-7166

Scott@EvidenceSolutions.com

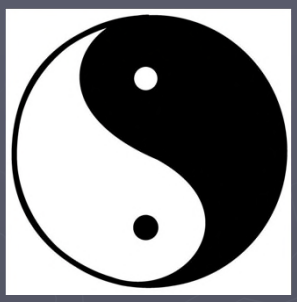
Protecting Electronic Medical Record Systems - Digital Information Security For Health Care Providers

Faculty:
Scott Greene
of
Evidence Solutions, Inc.

Scott@EvidenceSolutions.com
www.EvidenceSolutions.com

- "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

Protect the Information



Provide Access

- If you want total security, go to prison. There you're fed, clothed, given medical care and so on. The only thing lacking... is freedom.
  - Dwight D. Eisenhower

You need to understand the enemy before you can defeat them.

Famous Hacking Events

- Back in 2004, a hacker managed to break into Microsoft's corporate network and stole the source code for Windows 2000, about 600 million bytes of data, posting it online. The hacker was never caught.

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

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

Seven Threats

- 1. Recon
  - Goal: to learn about vulnerabilities in the targeted network and systems, including credentials, software versions, and misconfigured settings.
    - Social Engineering
      - Fools end users into surrendering data.
    - Phishing / Spear Phishing
    - Pharming (fraudulent web sites)
    - Drive-by pharming (redirected DNS on hijacked wireless access points).

Seven Threats

- 1. Recon
  - Websites & other public facing content
  - Email addresses
  - Social Media
    - Personal
    - Professional

Seven Threats

- 1. Recon
- Countermeasures:
  - Employees: "If you see something unusual, tell someone!"
  - Partners / Associations: "Share Share Share!"

Seven Threats

- 2. Lure
- Using information from Recon Stage:
  - Cybercriminals create socially engineered:
    - Email
    - Social Media Posts
    - Text messages
    - Web pages
      - That cause users to act in ways that seem in their self-interest but in reality lead them astray.

Seven Threats

- 2. Lure
  - Users fall for:
    - Disaster related material
    - Social drama
    - Celebrity deaths or gossip

Seven Threats

- 2. Lure
  - Watering hole attack:
    - Silent – The attacker compromises a high-traffic site and relies upon its existing, legitimate content to entice users to act.
      - In 2013: NBC.com
  - Users feel secure going to well known sites.
  - Cybercriminals take advantage of that sense of security
  - Generally these are sites users visit daily

Seven Threats

- 2. Lure
  - Fox News – Current Events:
    - Activity in Syria
    - Immigration Reform
    - War on Terror

Seven Threats

- 2. Lure
  - Countermeasures:
    - User Education
      - Is it grammatically correct?
      - Hover over the link – does it go where you think it is supposed to go?
      - Warn Users: "We are seeing lots of email about……"

Seven Threats

- 3. Redirect
  - Yahoo experienced this kind of attack in early 2014.
  - There were up to 27,000 redirects happening per hour
  - Millions of users were affected
  - All due to an Ad server that was compromised and displayed ads that were redirected
  - Users were caught unaware – Yahoo is trusted

Seven Threats

- 3. Redirect
- Sources

1.Web and email spam	**6.Information technology**
2.Sex	**7.Shopping**
3.Hacking	**8.Travel**
4.Illegal or questionable	**9.Entertainment**
5.Business and economy	**10.Advertisement**

Seven Threats

- 3. Redirect
- Countermeasures
  - Products that provide real-time awareness of both web page reputation and redirect destination
    - DNS
    - Filtering

Seven Threats

- 4. The Kit
  - Kits generally look for zero day vulnerabilities
    - Cybercriminals are lazy they seek weaknesses that can open doors for delivering:
      - Malware
      - Key loggers
      - Other tools
    - This enables them to further infiltrate networks and steal data or compromise additional systems.
    - The strive to stay ahead of updates

Seven Threats

- 4. The Kit
  - 2013 Blackhole
    - Deployed using Java
    - When released an estimated 94% of browsers were susceptible
    - One month after the patch adoption was only 7 percent.
    - One year later 31% of systems were still un-patched

Seven Threats

- 4. The Kit
- Countermeasures
  - Patch patch patch

Seven Threats

- 5. Dropper File
  - The dropper file is code, once delivered and installed on a system, enables the attacker to persist and advance an attack.
  - The code morphs – Antiviruses don't see it
  - The attacker as gained control
    - Disabling antivirus
    - Disabling Firewalls

Seven Threats

- 5. Dropper File
  - Cryptolocker
    - Profit by preventing access to user's data.

Seven Threats

- 5. Dropper File
- Countermeasures
  - Real-time defenses – still detect some drops
  - Site reputations
  - Signature checks

Seven Threats

- 7. Theft of data
  - Theft of data or destruction of data
  - Gain of Intellectual Property
    - Blackmail
    - Sell on black market for financial gain
  - Invisible delivery:
    - Dropbox, Box, Google Drive

Seven Threats

- 7. Theft of data
- Countermeasures
  - See 1 through 6….
  - Difficult to detect.
  - Data drip – slow exfiltration of data
  - Data Loss Prevention (DLP)

Threat Status

- Dell
  - http://www.secureworks.com/cyber-threat-intelligence/cyber-security-index/

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.

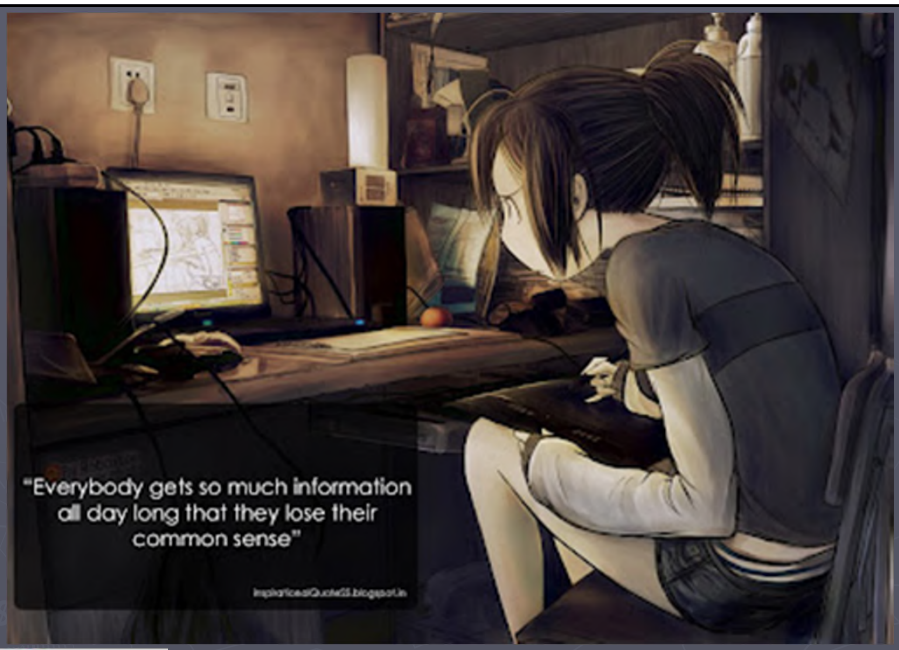
Famous Hacking Events

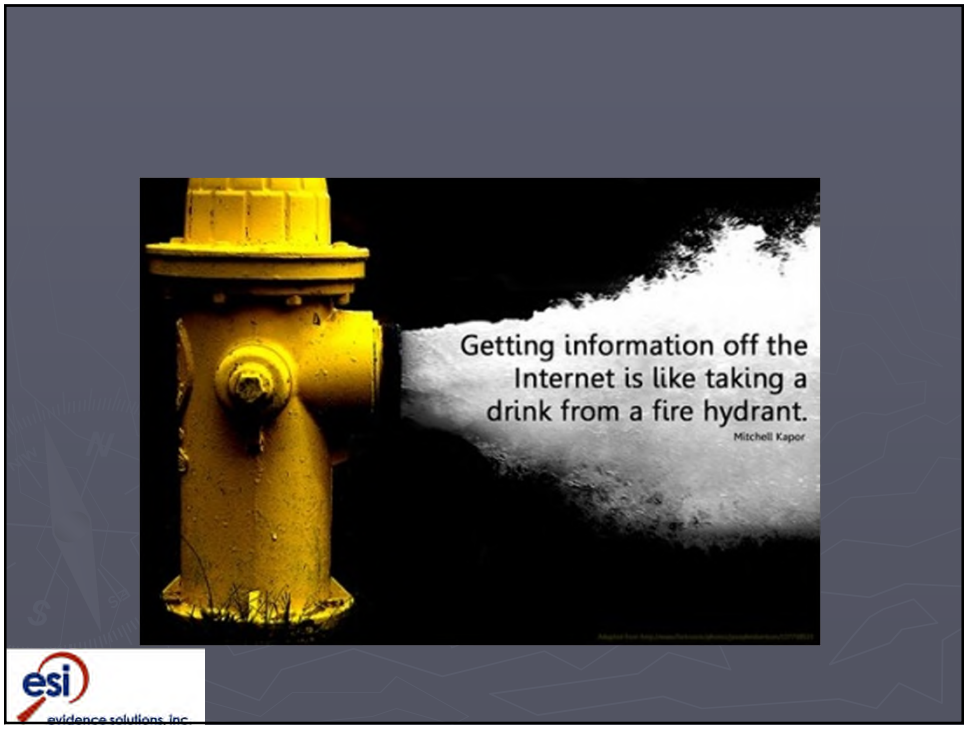
- Operation Get Rich
  - Alberto Gonzalez wanted money
  - From 2005 to 2007 he and his crew used SQL injections to steal 170 million ATM and credit card numbers
  - They were collected from retailers like TJ Maxx, DSW and Dave & Buster's.
  - The crew then sold them at auction Gonzalez a tremendous profit.

Famous Hacking Events

- Operation Get Rich
  - Before he was jailed, he told the judge in his case he was working undercover for the Secret Service.
  - He ended up getting 20 years in jail.

In October 2006, a foreign hacker broke into a system at a water-filtration plant in Harrisburg, Pa., after an employee's laptop computer was compromised via the Internet and then used as an entry point to install malware on the plant's computer





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 Engineering

- Methods
  - 1) call help desk to find out the secret questions with a non target
  - 2) They gather up the target's secret question answers.
  - 3) once they have that they get the help desk to change the password
  - 4) then they call the target and inform them about the change

Social Engineering

- Methods
  - give out usb flash drive with malicious code
  - get a keylogger with bluetooth

Social Enginering

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

Events & Social Engineering

- In the last couple of years:
  - Malaysian Airlines MH370
  - Boston bombing
  - Hurricanes
  - Tornados
  - The World Cup

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

- 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.

Resources

- Microsoft's Web Application Configuration Analyzer (just released 2.0)
  - Scans IIS servers
  - Hosted applications
  - SQL Server instances for common security issues and mis-configurations.

Resources

- Foundstone (a McAfee organization)
- Google diggity
- Bing diggity
- Stach & Liu used Google trends:
- Stachliu.com/index.php/resources/tools/googlehackingtools

Resources

- Free Windows rootkit detection tools:
  - Sysinternals Rootkit Revealer
  - Avast! Antivirus
  - Sophos Anti-Rootkit
  - F-Secure Blacklight
  - MalwareBytes
  - HijackThis
  - Kaspersky removal tool

Resources

- Infragard
- NIST
- SANS

Resources

- True Crypt Alternatives
  - VeraCrypt (TrueCrypt) - Windows, Android, Mac
  - CipherShed (TrueCrypt) - Windows
  - TCnext (TrueCrypt) - Windows
  - AES Crypt - Windows, Mac, Android, iOS
  - AxCrypt - Windows
  - DiskCryptor - Windows
  - EncFS - Windows, Linux, Android (Mac)

Contact Information

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

Evidence Solutions, Inc.

Biography

Scott Greene

Scott is the CEO of Evidence Solutions, Inc. Scott Greene has been doing Data Recovery, Computer, Technology and Digital Forensics, and EDiscovery work for over 30 years.

Directly out of high school, Scott went to work for IBM as a programmer.

In 2008 he created Evidence Solutions, Inc., a full service Computer, Technology & Digital Forensics firm, from the Technology Forensics department of Great Scott Enterprises.

Scott has developed and presented strategic planning seminars, taught numerous classes in database design & optimization, cyber security and technology forensics. Scott's extensive knowledge draws clients to him from all over the United States as well as Internationally for consulting and expert witness services in the field of Technology, Computer & Digital Forensics. His extensive and diverse experience allows him to be an expert in many facets of computer & digital technology.

Scott and Evidence Solutions have been involved in Civil & Criminal Cases, for Plaintiff, Defense and Special Master in Justice, Superior & District Courts as well as Internationally.

He is a sought after speaker and educator and travels throughout the country presenting to local, regional, national and International organizations.