


What County Officials, Management and Staff Should (or Shouldn't) Know About Technology



June 17, 2010



- You and Awareness
- Perimeter Security
- Cyber Security
- Summary & Questions




June 17, 2010


Technology, Terrorism, Security and You




Who Is Responsible For Security?



- Not the local Police
- Not the Sheriff
- Not the State Police
- Not Government
- Not IT





Questions



- Honestly did you really see the Bear?
- Are you aware of your surroundings?
- Do you see what is going on around you?
- Do you walk with authority or schlep along?
- Are you looking up or down when on your cell phone?
- Are you a target????????????????????

OODA Loop

```

    graph TD
      Observation((Observation)) --> Orientation((Orientation))
      Orientation --> Decision((Decision))
      Decision --> Action((Action))
      Action --> Observation
  
```

OODA Defined

Observation	Orientation	Decision	Action
• Collect the inputs/data of the situation.	• Analyze the inputs/data to determine your position.	• Determine your course of action.	• Execute your decision.

Risk Management Approach

Many organizations have approached security risk management by adopting the following:

Reactive approach	Employ a process that responds to security events as they occur
Proactive approach	Implement a process that reduces the risk of new vulnerabilities in their organization

Risk Assessment Attributes

Asset → Threat → Vulnerability → Mitigation

Security Risk Assessment

Asset What are you trying to protect?	Threat What are you afraid of happening?	Vulnerability How could the threat occur?	Mitigation What is currently reducing the risk?
Impact What is the impact to the organization?		Probability How likely is the threat given the controls?	
Well-Formed Risk Statement			

Terrorism Defined

Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

FBI Definition

Access Controls

Locks

Common Security Biometrics

- Finger Print Scan
- Hand and Finger geometry
- Facial Recognition
- Speech Verification
- Signature
- Retina Scan
- Iris Scan

Perimeter Security






Five Camera Considerations

- 1 • Field of View
- 2 • Lighting
- 3 • Frame Rate
- 4 • Resolution
- 5 • Focus





Terrorist Acts

VBIED Wall Street 1920

Bomb Components

				
Container	Charge	Power	Detonator	Switch

Home Made Chemical Bomb

-  Water Bottle
-  Tang Drink Mix
-  Hydrogen Peroxide
-  Disposable Camera

Cyber vs. Physical Attack Differential

- May not be seen
- Physical could be accidental
- Cyber is never a accident

What does Cyber touch/affect?

- Critical Infrastructures
 - Emergency services
 - Power
 - Water
 - Gas & Oil
 - Banking and finance
 - Transportation
- Industry and Military
- Our homes, offices and schools
 - In Short – just about everything!


2007 Major Cyber Attack

- Systems Broken Into
 - Department of Defense
 - Department of State
 - Department of Commerce
- Probably
 - Department of Energy
 - NASA
 - All Military Agencies

They went undetected for several days.

Downloaded Terabytes of Data.

Terrorist Targets

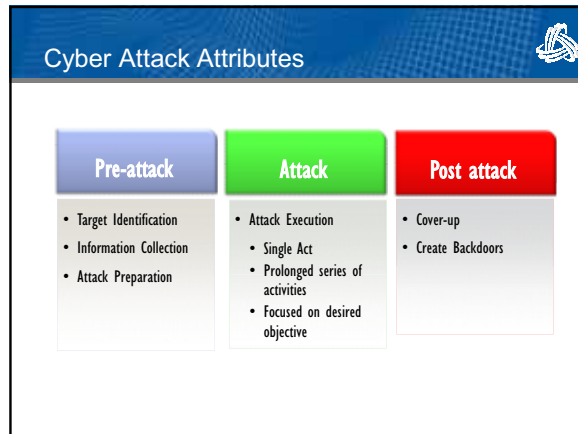
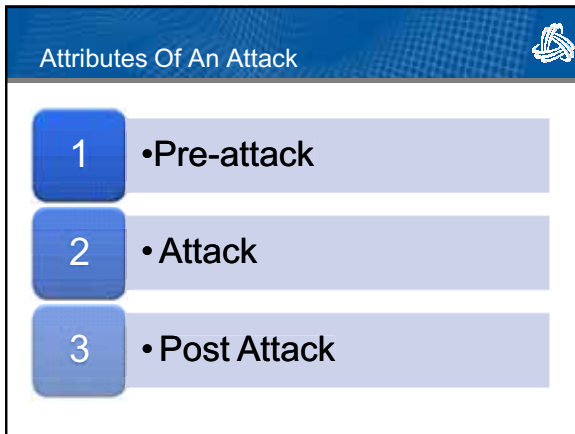


Infrastructure

Cyber Perimeter Security

- Must have
 - Firewall
 - VPN
 - Intrusion Detection System (IDS)
 - Anti-virus
 - Content Filtering
 - Log Review
 - DMZ
 -

You need to protect everything inside the perimeter!



- ### Unstructured Threats
- Individual/small group (script kiddies, piracy groups) with little or no organization or funding.
 - Easily detectable information gathering.
 - Exploitations based upon documented software flaws and published exploit code.
 - No specific target; target of opportunity, may not know who/what is being attacked.
 - Motivated by thrills, bragging rights, access to resources, etc.
 - Goal may be to gain control of computers for other purposes.

- ### Structured Threats
- Well organized (organized crime, hackers, espionage), planned and funded.
 - Specific targets and employ extensive information gathering to optimize path and means of attack.
 - Goal – data stored on the systems or computers themselves.
 - May rely on insider help or unknown system and application flaws.

- ### Highly Structured Threats
- Extensive organization (nation-states, terrorists), funding, and planning, over and extended time, with the goal of having an effect beyond the data or computers attacked.
 - Stealthy information gathering.
 - Multiple attacks/types of attacks, exploiting previously unknown flaws, possibility with insider help.
 - Coordinated efforts from multiple groups.

Malware Defined



A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim.

Malware



- Virus
- Worms
- Trojan
- Spyware
- Loggers
- Bugbot
- Botnet
- Click jacking
- Mic-jacking

Low Price of Admission



- \$150 - \$500: List of 5,000 computer address infected with spyware and are waiting to be remotely controlled as part of a automated Bot Network.
- \$1000 - \$5000; Information about computer vulnerabilities for which no software patch yet exists.
- \$95 - \$225 for Botnet software and \$4500 for the entire catalog and they guarantee the bots will never be detected.

Ground Zero For The Web Is The Internet



Trojans



Botnets



Scareware

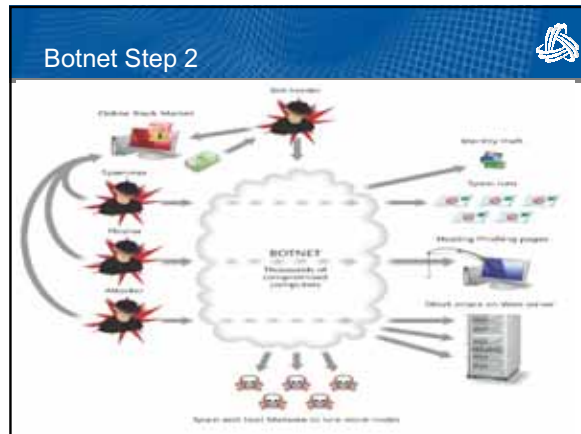
Trojans



- Most common downloader malware to get hit with on the Web.
- It always pretends to be something else.
- A good Trojan will not slow your computer down.
- It will probably symptom free.
- There is no safe web page.
- Just looking at the infected web page and Bang!
- It can be the silent killer.

Botnet





- ### Scareware
- The third and arguably most irritating leg of the malware stool.
 - Fake antivirus programs.
 - Ultimate no win situation.
 - Will not go away. (Alt-Control-Delete)
 - If you pay you become another warrior on the scammer's botnet army.

- ### Attack Motivators
- Vendetta/Revenge
 - Joke/Hoax/Prank
 - The Hacker's Ethics - This is a collection of motives that make up the hacker character
 - Terrorism
 - Political and Military Espionage
 - Hate (national origin, gender, and race)
 - Fame/Fun/Notoriety
 - Personal Gain



- ### More Vulnerabilities
- Wireless connections
 - 3rd Parties
 - Contractors
 - People taking data home
 - Laptops
 - Working from home
 - General Packet Radio Service (GPRS)
 - Guests
 - Malware

Social Networking Sites



- Are they safe?
- Should you be able to access social networking sites from your County computer?
- Social Networking Sites have become a fertile playground for hackers.
- Participants that sign on to these sites need to think about what personal information they post.

Smart Phone Vulnerability



Smart Phone Do's



- Only deploy devices that support features like encryption, remote wipe, and password locking.
- Create specific security policy and procedure items for mobile devices that govern acceptable use and responsibilities.
- Ensure devices in the field can be updated quickly to fix security issues.
- Define what level of support you plan to provide if implementing different types of smart phones.
- Define the purpose of having a smart phone.

Smart Phone Don'ts



- Deploy devices for enterprise use without proper protections and control.
- Assume that all devices treat things like encryption the same way.
- Deploy devices without understanding what policies you have (or not) enabled and what your risk of data loss is.
- Allow unmanaged devices to access and retrieve data.
- Permit access to download applications.
- Blocking is not the keyword, controlling is.

Password Tips



- 1 • Never provide your password over email or in response to an email request.
- 2 • Do not type passwords on computers that you do not control.
- 3 • Do not reveal passwords to others.
- 4 • Protect any recorded passwords.
- 5 • Use more than one password.

Avoid Creating Passwords Using:



- 1 • Dictionary word in any language.
- 2 • Words spelled backwards, common misspellings, and abbreviations.
- 3 • Sequences or repeated characters.
- 4 • Personal Information

Strong Password

- Keys to password strength
 - Length
 - Complexity
- Whenever possible use at least 10 characters or more.
- The greater the variety of characters in your password the better.
- Use the entire keyboard, not just the letters and character you use or see most often.

Create A Password You Can Remember

- Start with a sentence.
 - Think of something meaningful to you.
 - Long and complex is better. (My first dance with Jean was 16 Candles by the Crests.)
- Turn your sentence into a row of letters.
 - Use the first letter in each word.
 - MfdwJw16CbC.
- Hint – Pet
 - TfplhwawSTnB:+

Brief Revisit Of This Vulnerability




Summary

- Deliver security information that users will view as being valuable to them personally and professionally
- Communicate with users, let them know why policies exist and why they are enforced for everyone
- Be mindful of security solutions that can impact usability and communicate the need to users whenever such solutions are implemented
- Remember that security awareness isn't a one shot fix but a long term process designed to educate AND to change user behavior



- You and Awareness
- Perimeter Security
- Cyber Security
- Summary & Questions

Thank You For Attending & Be Safe



June 17, 2010