APCO International
Leaders in Public Safety Communications™

APCO Emerging Technology Forum

PUBLIC SAFETY CYBER SECURITY

John Facella, P.E., C. Eng.
Senior VP, RCC Consultants

3 December 2013

Agenda

- “It Won’t Happen to Me”
- Issues in Cybersecurity
- What to do Right Now
- Summary
- Resources

The Threat is Real, Every Day, Every Hour

November 2013:
FBI: Anonymous hackers have been accessing government computers for almost a year and stealing information

November 20, 2013
Cupid Media Data Breach
Affects Millions of Accounts

Feb. 19, 2013
Mandiant Releases Report Exposing One of China's Cyber Espionage Groups

141 victims since 2006, terabytes of data

April 4, 2013
ALABAMA DEPARTMENT OF HOMELAND SECURITY Director Details Possible Personal Information Compromised in Cyber Intrusion of State IT System

November 14, 2013
Attacks on Healthcare.gov
Site Under Investigation

Feb. 27, 2013, DHS:
Chinese targeted 23 US natural
Gas pipeline operators Dec 2011 to June 2012

March 13, 2013
APCO reports Denial of
Service Attacks on PSAPs

March 2013
US Director of National Intelligence:
'There is a remote chance of major cyberattack on US critical infrastructure in next 2 years that would result in long-term, wide scale disruption.'

Per Mandiant

- 243 days = median time before advanced attackers in the network are detected
- 46% of compromised machines have no malware
- 100% of compromised machines have antivirus software
- 100% of breaches involved stolen credentials

Source: www.mandiant.com

Per Verizon's 2013 Data Breach Report

- 66% took months to discover
- 92% of breaches perpetrated by outsiders
- 76% exploit weak/stolen credentials; 29% leverage social tactics
- 96% of espionage cases attributed to China
- 95% of state espionage used phishing
- 70% of breaches discovered by 3rd parties

Source: http://www.verizonenterprise.com/DBIR/2013/

CyberArk

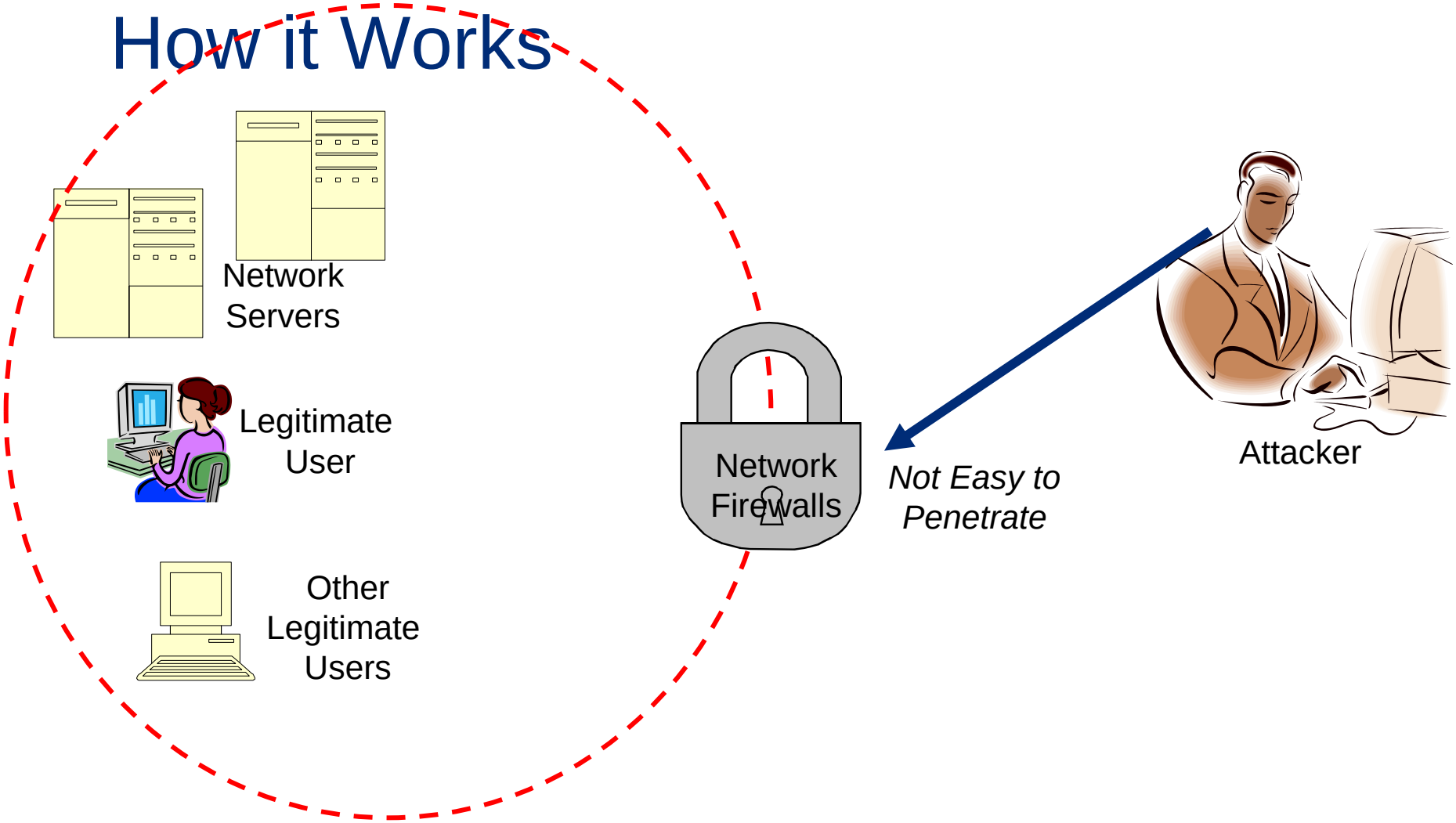
- Privileged Passwords in Critical Systems can be a problem

- Surveyed nearly 1,000 global executive and IT security professionals
  - 80 % consider cyberthreats a greater risk to their country than physical attacks

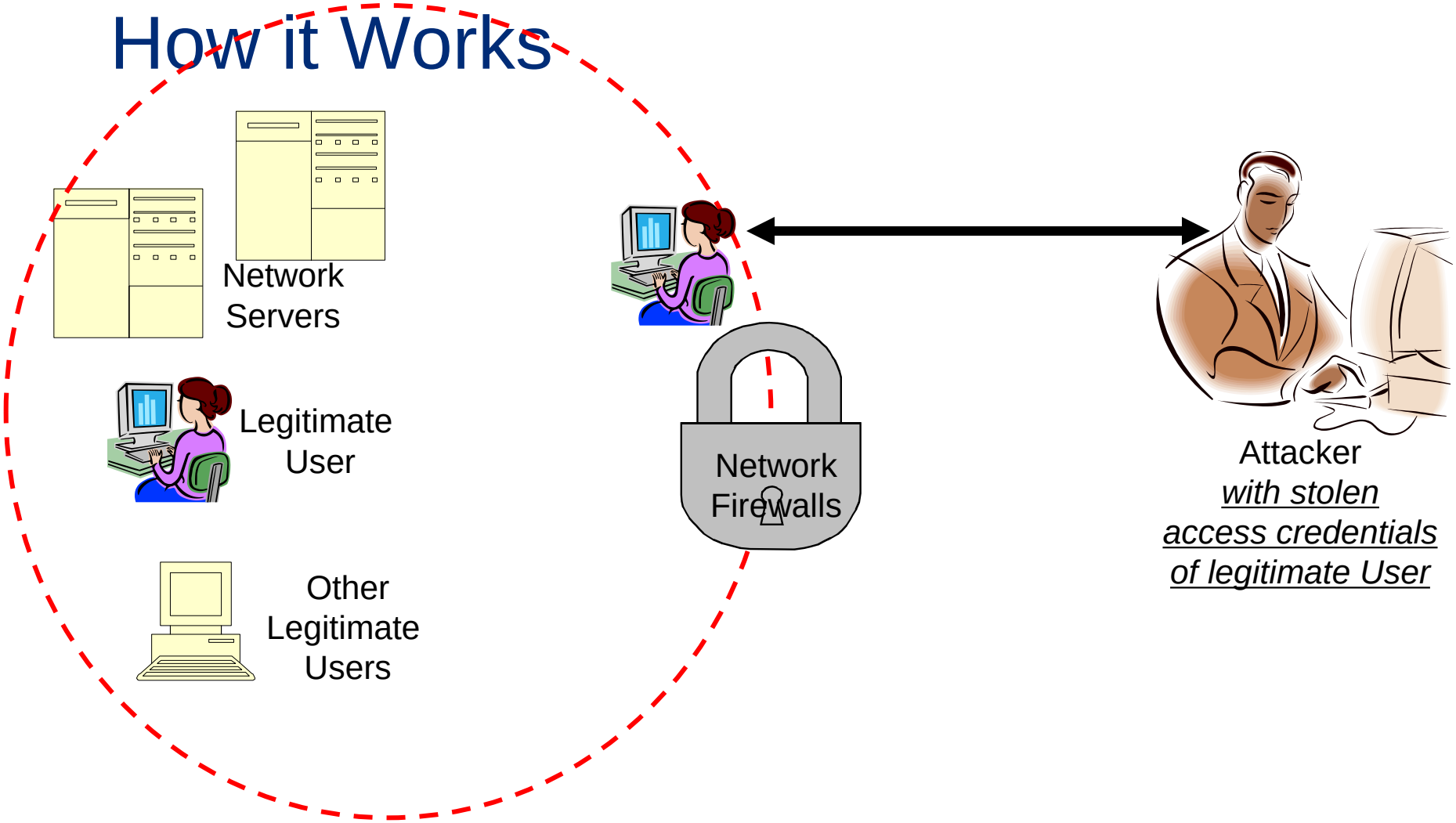
  - 51% believe that a cyberattacker is currently or has infiltrated their corporate network *within the past year*

Source: http://cyberark.com

How it Works


Network Servers
Legitimate User
Other Legitimate Users
Network Firewalls
Not Easy to Penetrate
Attacker

How it Works


Network Servers
Legitimate User
Other Legitimate Users
Network Firewalls
Attacker
with stolen access credentials of legitimate User

Common Themes

- Attacker gains legitimate user credentials
  - Circumvents most “Defense in Depth” protections like firewalls, closed backdoor ports, etc.
  - Only clue will be what they do while masquerading (abnormal behavior for that user)

- Discovery takes months

Agenda

- “It Won’t Happen to Me”
- Issues in Cybersecurity
- What to do Right Now
- Summary
- Resources

These Issues are Not New

- 1970: Report of the Defense Science Board Task Force on Computer Security, Chairman Willis Ware:
  - "It is important to influence designers of future computers and software *so that security controls can be installed before the fact and as an integral part of the system.* It is also important to ascertain what can be done with equipment presently installed or owned by the government."
    http://csrc.nist.gov/publications/history/ware70.pdf (from SANS Newsbites 26 Nov. 2013)

- 1989: "The Cuckoo's Egg" by Cliff Stoll

Some Issues Very Difficult to Deal With

- Fake Computer Chips
  - See IEEE Spectrum October 2013, pgs. 40-45
- Chips with hidden security flaws
  - "The majority of application-specific integrated circuits are manufactured outside the United States....People could be putting flaws in these chips that they can activate." Jim Howard, director and chief engineer of information assurance at L-3 Communications
  - (IEEE Spectrum 6 Jan. 2010, "Creative Winners in Hardware Trojan Contest")

Why the Cyber threat to the PSBN is Different & Unprecedented

- Silos removed on >50K public safety communications systems = *massive increase* in threat actor reward

- Large number of threat actors:
  - Nation-states
  - Terrorists
  - Corporate Espionage
  - Criminals
  - Hacktivists (e.g., Anonymous)
  - Disgruntled employees
  - Nuisance & thrill seekers

Why the Cyber threat to the PSBN is Different & Unprecedented

- Multiplicity of user agencies = varying policies, resources, regulations
  - Federal, state, local
  - Law enforcement: sheriffs, police, state police, state patrol
  - Fire: career, combination, part-time, volunteer and paid-on-call
  - EMS: fire based, hospital based, volunteer, private ambulance (HIPAA)
  - Utility companies, transportation agencies??

- The PSBN will be a complex network of eNode B base stations, servers and gateways, passing terrabytes of data

- Bring Your Own Device (BYOD)

- Bring Your Own Application (BYOA)

Image: Blogs.Norman.com

Emerging Threat Trends

- It's beyond Denial of Service Attacks, which in fact may mask 'real attacks' harder to detect
- Digital certificate structure is now suspect
- Traditional blacklisting based on signatures inadequate
- Attacks appearing that neuter defense capabilities (e.g., anti-forensics, misattribution of malware)
- Advanced Persistent Threats (APT) growing

Emerging Threat Trends

- Horizontal mechanisms that impact multiple assets simultaneously (e.g., the cloud)
  - Cloud based computing has serious security implications, yet many agencies are moving toward it to save $

- New Technologies (e.g. new HTML5 web specification includes device geolocation)

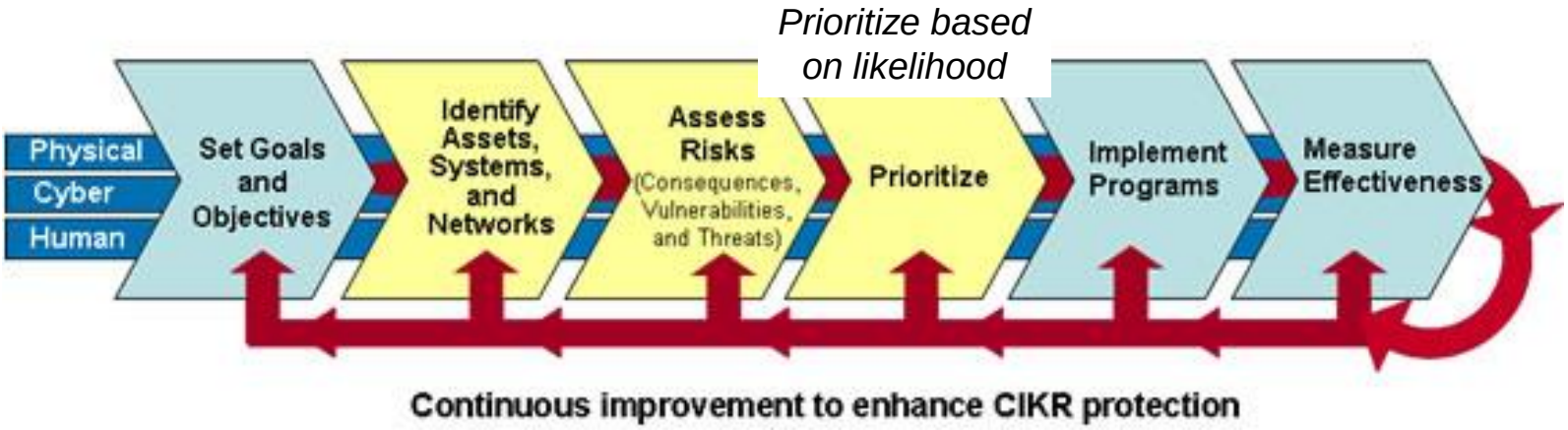
Changing Our Approach

- Move from compliance models, ‘frameworks’, and ‘risk management’, to *actively fixing security flaws*

- Continue prevention (“defense in depth”) but *must* add prediction, detection, response, intelligence capabilities
  - Benchmark time to detection and time to mitigation
  - Defensive, reactive only solutions inadequate

Security Risk Management

National Infrastructure Protection Plan Risk Management Framework



Source: www.dhs.gov/homeland-infrastructure-threat-and-risk-analysis-center

Agenda

- “It Won’t Happen to Me”
- Issues in Cybersecurity
- What to do Right Now
- Summary
- Resources

What to Do NOW

- Educate Users to the threat of Phishing Attacks
  - Introduce DHS' "Stop-Think-Connect" program
- Implement and Enforce Policies on:
  - Forced Periodic Password changes
  - Strong Passwords (phrases including special characters, easy to remember)
  - Use of Thumb Drives
  - VPNs
  - Strangers Using Agency Computers
  - User Supplied Devices (BYOD)
  - User Supplied Applications (BYOA)
- Implement the first 4 SANS Critical Security Controls, and plan to implement the next 4 soon

Agenda

- “It Won’t Happen to Me”
- Issues in Cybersecurity
- What to do Right Now
- Summary
- Resources

Summary

- Security is a continuous journey, and measures/countermeasures are constantly changing
  - You will never be 100% secure
  - Constant vigilance needed
  - Difficult to 'add on' security
- Bad guys are getting 'badder'
  - Move focus to fixes from compliance reports
  - Traditional "Security in Depth" no longer enough
  - Single solution/vendor inadequate
- Public Safety and the FirstNet PSBN system will represent a unique target to defend, and needs careful thought on how to implement security measures, some of which may not exist today
- There are measures every agency can start taking, RIGHT NOW
  - Stop-Think-Connect
  - The first few SANS Critical Controls

Agenda

- “It Won’t Happen to Me”
- Issues in Cybersecurity
- What to do Right Now
- Summary
- Resources

Resources

- UTC Journal, 1st Quarter 2013 (devoted to Cybersecurity)
- Verizon *2013 Data Breach Investigations Report*
- *CyberWar*, Richard A. Clarke, Harper Collins, 2010
- Mandiant report on China's hacking organization, www.mandiant.com
- SANS Newsbites
- SANS 20 Critical Security Controls: www.sans.org/critical-security-controls
- NPTSC BB Security Working Group white paper
- NFPA 1221, 2013 edition, Chapter 13 Data Security, and proposed Chapter 13 for 2016 edition

Resources

- Homeland Security Newswire: www.homelandsecuritynewswire.com/topics/cybersecurity
- www.dhs.gov/stopthinkconnect
- IACP Cyber Center: http://www.iacpsocialmedia.org/Portals/1/documents/fact%20sheets/cyber%20center%20fact%20sheet.pdf
- FBI's Cyber Shield Alliance
- RCC's NIST cybersecurity white paper: www.rcc.com/resources/archive/04-08-2013-RCC-NIST-Cybersecurity.pdf

Q & A

Follow APCO at…

facebook.com/apcointernational

@apcointl

Thank You!

John Facella
jfacella@rcc.com