At Risk: Increasing Cyber Threats

Dawn Roth Lindell

August 2015

Western AREA POWER ADMINISTRATION

2014 Cyber Attacks

January- April: ICS-CERT Monitor cites three incidents:

- Unnamed public utility control system hacked
  - Internet facing
  - Weak password/brute force susceptible
- Unprotected, internet connected control system operating a mechanical device
  - Control system server accessed via cellular modem
  - Extended period of time
- Sochi HVAC System
  - Internet connected
  - No authentication required

INDUSTRIAL CONTROL SYSTEMS
CYBER EMERGENCY RESPONSE TEAM

Western AREA POWER ADMINISTRATION

2014 Cyber Attacks

April: Heartbleed

- 17% (around half a million) of the Internet's secure web servers believed to be vulnerable to the attack
- Allowed theft of the servers' private keys and users' session cookies and passwords
- Western – 67 vulnerabilities identified and corrected

May: Five Chinese nationals indicted for computer hacking and economic espionage. Targets included Westinghouse Electric (energy and utilities)

Western AREA POWER ADMINISTRATION

2014 Cyber Attacks

June: Ugly Gorilla hack of Northeastern U.S. Utility exposes cyberwar threat

- State sponsored by China
- Stole schematics of pipelines
- Copied security-guard patrol memos
- Sought access to systems that regulate the flow of natural gas.
- Cruised channels where keystrokes could cut off a city's heat, or make a pipeline explode

September: Chinese hackers blamed for intrusion at energy industry giant Televent

Western AREA POWER ADMINISTRATION

2014 Cyber Attacks

September: Shellshock/Bashdoor

- Internet facing
- Allows attacker to execute arbitrary commands
- Attacker can gain control over system
- 55% of attacks executed within China and US
- Distributed Denial of Service
- Vulnerability scanning
- Millions of unpatched servers at risk

Western Area Power Administration

2014 Cyber Attacks

October: Black Energy (published by Kaspersky Lab)

- Converted crimeware tool
- Operates plug-ins for Linux and Windows
- Cloud based ICS systems at risk
- Used to attack networking devices, steal digital certificates
- Can brick systems it infects and skillfully hide from security analysts.

Western AREA POWER ADMINISTRATION

2014 Cyber Attacks

December: Sony hacked by North Korea

- Destructive malware deployed
- Destroyed systems
- Stole employee Personally Identifiable Information (PII)
- Stole proprietary information
- FBI called within hours

December: Christmas hack of Sony PlayStation Network and Xbox Live

Western AREA POWER ADMINISTRATION

DOE Cybersecurity Risk Information Sharing Program

- **December**: A report analyzing cyber threats from January through September 2014
- Concluded that cyber threats to critical infrastructure are real and increasing
- Noted at least eight groups in the Middle East, Asia and Europe targeting the electric sector.

U.S. DEPARTMENT OF ENERGY

Western AREA POWER ADMINISTRATION

2015 Cyber Attacks

March:

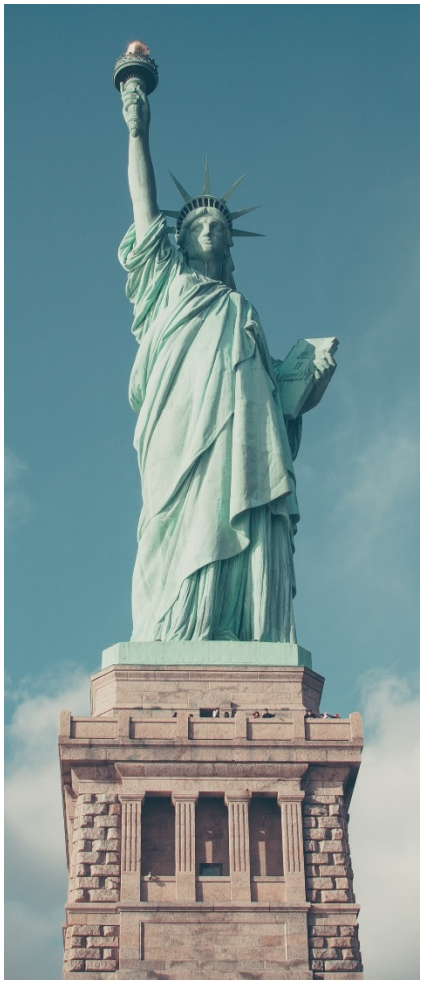
Primera Blue Cross

- 11 Million customers affected
- Intruders entered on May 5th
- Discovered on January 29 – 274 days
- Names, addresses, SSN, e-mail, phone, bank accounts

USA Today article – Power Grid

- Physical and cyber attacks occur 1 in 4 days.
- Impact of a widespread outage
- 362 plus attacks since 2011
- Small and large utilities attacked

2015 Cyber Attacks



Federal Office of Personnel Management (OPM)

April: Personnel data of 4.2 million current/federal employees

June: Background checks of 19.7 million federal employees and 1.8 million spouses

- SSN
- Security clearance info

Utilized known vulnerabilities identified as early as 2008.

2015 Cyber Attacks

August:

IRS Hack

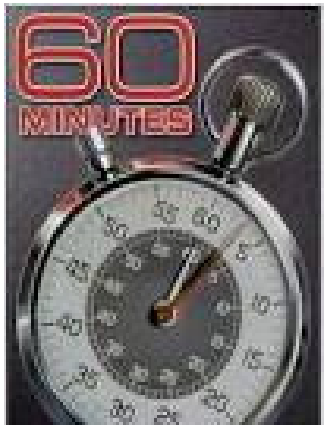
Ashley Madison Hack

Pentagon Computers – news identifies the Russians

Could this happen to you??

Answer: Of course it could!!

Western AREA POWER ADMINISTRATION



60 Minutes – November 30, 2014

- Fire Eye CEO Dave DeWalt
- “97% of all companies are getting breached”
- Hundreds of thousands each week
- 229 days on average from breach to discovery
- 80% of access is through stolen/weak passwords
- Cited Target Hack
  - Stole user name and password from vendor
  - Installed malware to steal credit card info

Western AREA POWER ADMINISTRATION

FBI Director, Robert S Mueller III

- “I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again. ”

Western AREA POWER ADMINISTRATION

Physical and Cyber Attacks

- "With the increased convergence of cyber and physical worlds, attacks are no longer limited to office computers and networks," says Steve Durbin, Managing Director of Information Security Forum. "They can now have physical impact in the real world."
- Western Area Power Administration
  - 37 physical attacks in 2014
  - Thefts
  - Reconnaissance
  - 650% increase in cyber incidents in last 3 years

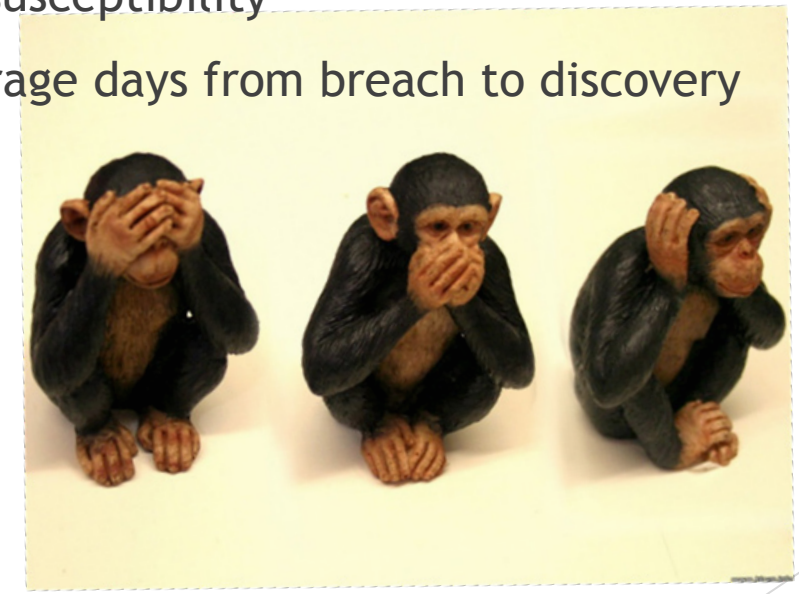
Western AREA POWER ADMINISTRATION

“So … what’s a girl (or guy) to do?”

Western AREA POWER ADMINISTRATION

Common themes

- Internet connectivity or wireless access
- Weak passwords
- Weak authentication
- Old tools, versions
- Internal threat
- Vendor susceptibility
- 229 average days from breach to discovery



Western AREA POWER ADMINISTRATION

Good security hygiene is critical

- Minimum: Strong passwords, changed quarterly
- Better: Multi factor authentication
- Remove, disable, rename default system accounts
- Implement account lockout policies
- Separate ICS network from business network
- Beware the mobile media device

Western
AREA POWER
ADMINISTRATION

Good security hygiene is critical

- Focus on the employees – Insider Threat
  - Most often unintentional
  - And…..intentional threat is real
- Deliver employee training that is interactive and emotional
  - Anti-phishing campaign
  - Leadership training

Good security hygiene is critical

- Vendor Management
  - Require vendor security standards
  - Monitor creation of Administrator level vendors
- Apply patches
- Continuous monitoring
  - Standardize
  - Work to reduce alerts
- Complete a vulnerability assessment and address
- Intrusion Detection System
- Intrusion Prevention System

Western AREA POWER ADMINISTRATION

SANS Top 20 Controls -a good place to start

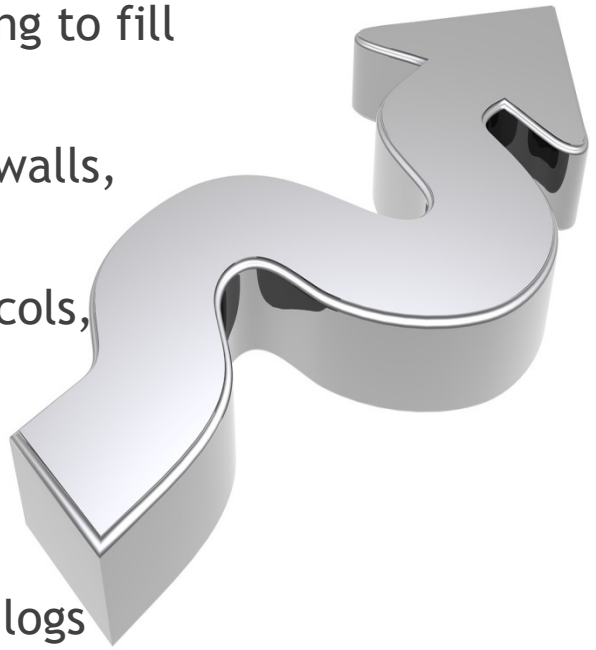
1. Inventory of authorized and unauthorized devices
2. Inventory of authorized and unauthorized software
3. Secure configurations for HW and SW on mobile, workstations,servers
4. Continuous vulnerability assessment and remediation
5. Malware defenses
6. Application Software security
7. Wireless access control
8. Data recovery capability

Security Skill assessment and appropriate training to fill gaps

Secure configurations for mobile devices – firewalls, routers, switches

SANS Top 20 Controls -a good place to start

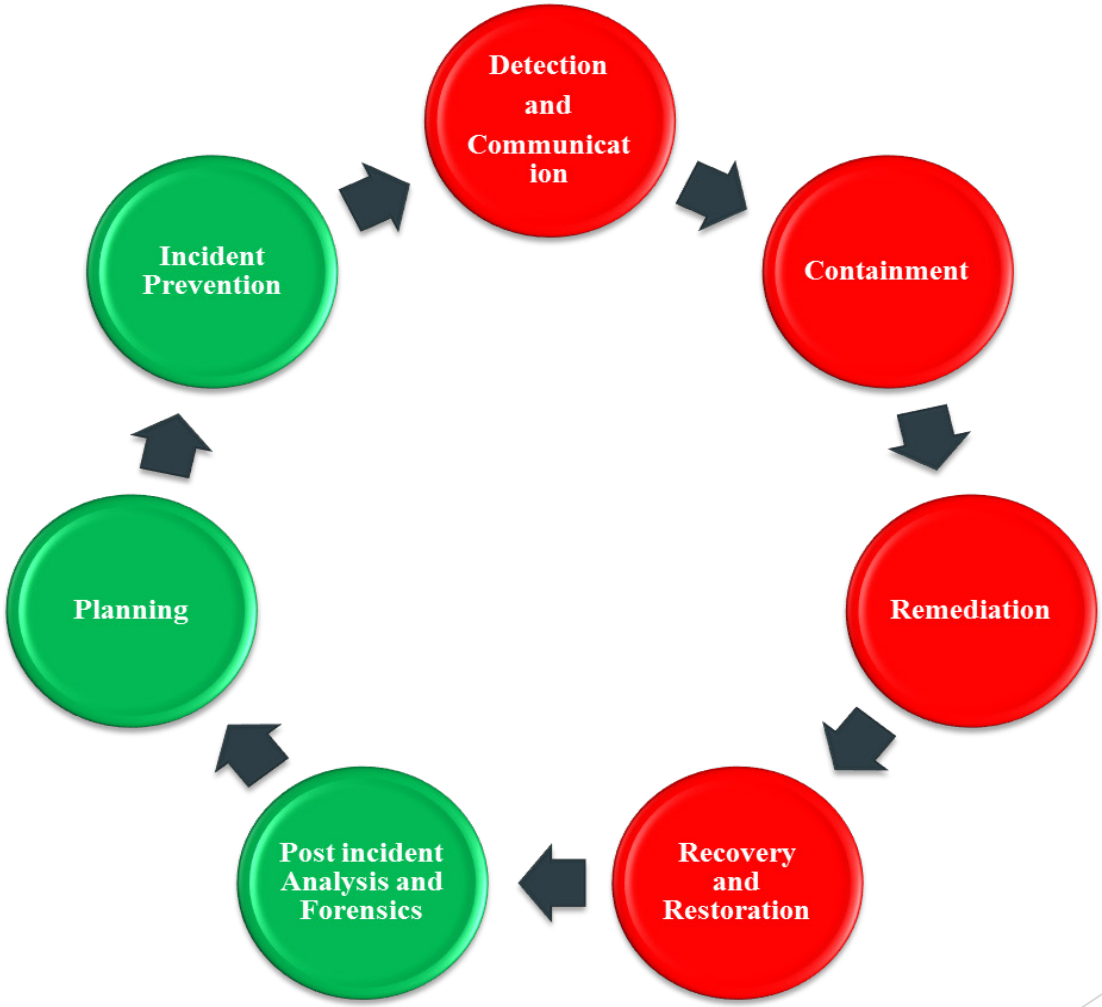
8. Data recovery capability
9. Security Skill assessment and appropriate training to fill gaps
10. Secure configurations for mobile devices – firewalls, routers, switches
11. Limitation and control of network ports, protocols, services
12. Controlled use of Administrative privileges
13. Boundary defense
14. Maintenance, monitoring and analysis of audit logs



SANS Top 20 Controls -a good place to start

15. Controlled access based on need to know
16. Account monitoring and control
17. Data Protection
18. Incident Response and management
19. Secure Network engineering
20. Penetration tests and red team exercises.

Intrusion Cycle



Partnerships

- Business from same sector
- Trade organizations
- User groups
- Regional Business Alliance

Western
AREA POWER
ADMINISTRATION

Western Cyber Exchange

- Public Private Partnerships – 3 states
- Brainchild of two Principles of Imprimus, Inc.
- Regional focus on cyber security
- IT users forum
- Training
- Data sharing – partnering with Mitre (Crits)

Western AREA POWER ADMINISTRATION

Governmental Partnerships

- FBI – Infragard
- Energy Sector – Information Sharing and Analysis Center (ES – ISAC)
- ICS-CERT

Western AREA POWER ADMINISTRATION

Information is Power

- Preparedness
- Defenses
- Monitoring
- Information sharing
- Rapid response

It isn't a question of "If"

Western AREA POWER ADMINISTRATION

Questions

Dawn Roth Lindell
Lindell@wapa.gov

Western AREA POWER ADMINISTRATION