

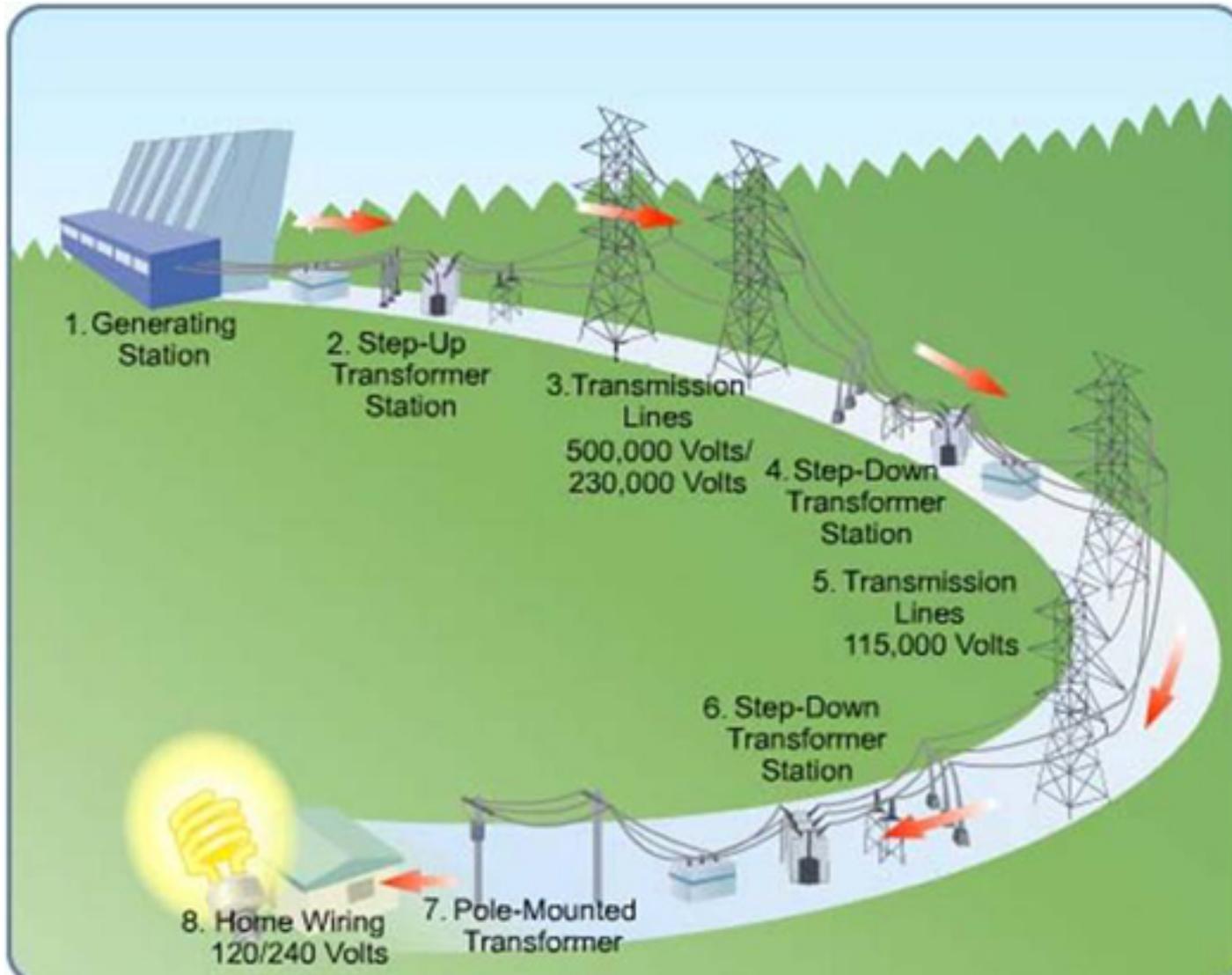
At Risk: Increasing Cyber Threats in the Electric Sector

Dawn Roth Lindell

January 11, 2016



Analyzing cyber risk on the grid



What happens when the power goes out - indefinitely?



But surely “they” can restore the power, right? Oh, and that is us!



Cyber attacks to date have not resulted in large outages

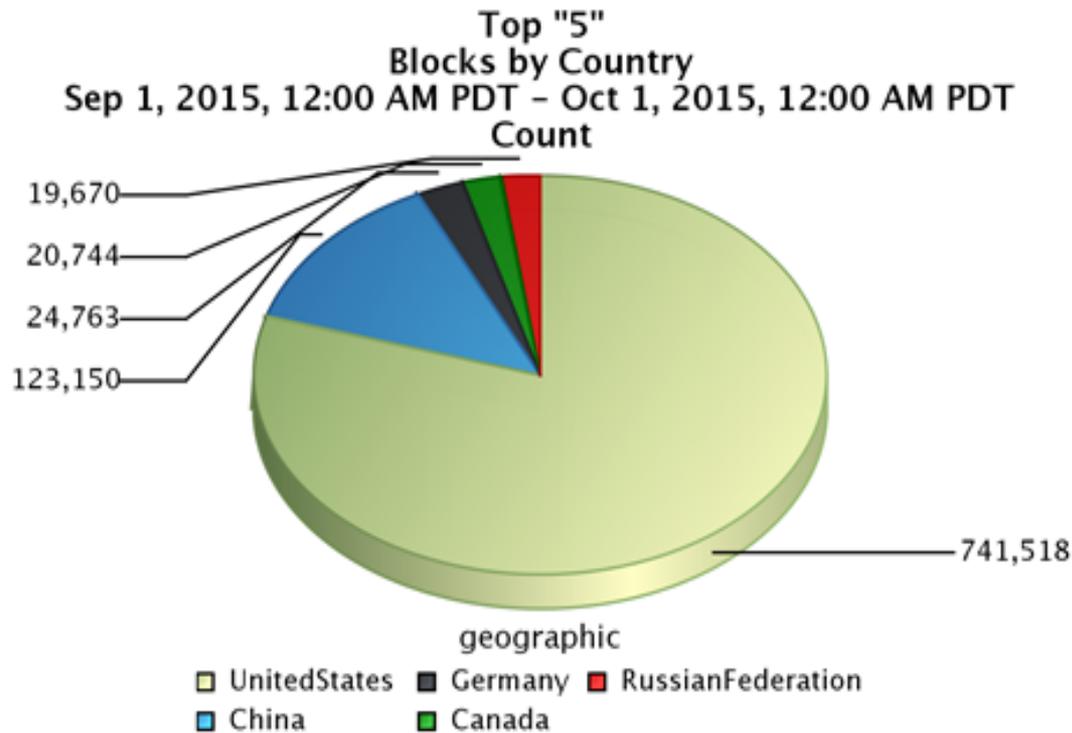
- ▶ The Chinese
- ▶ The former USSR nations
- ▶ US environmental extremists and anti government
- ▶ Friendly nations
- ▶ ISIL
- ▶ And then came the December 23, 2015 Ukraine attack



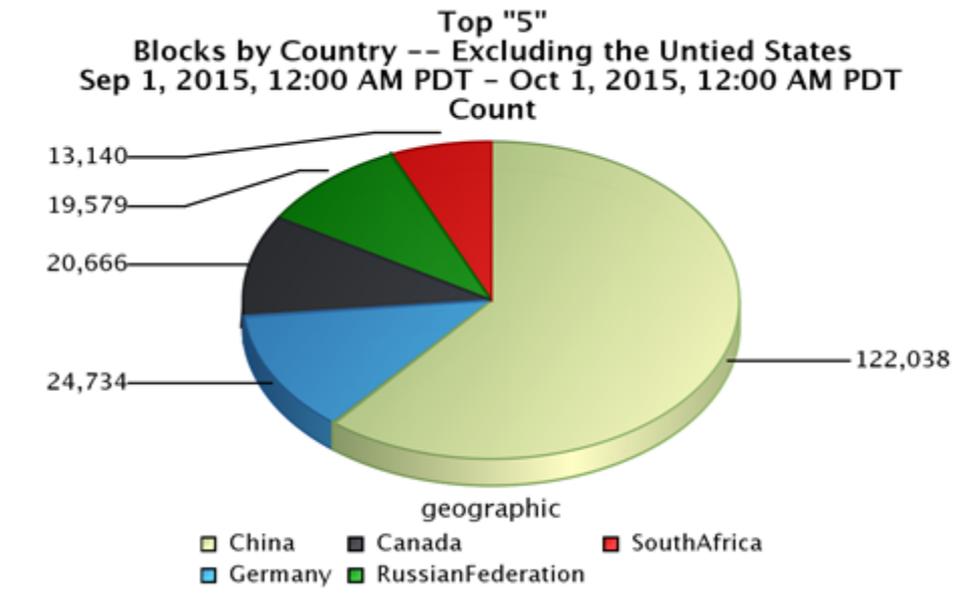
Analysis of the 12/23/2015 Ukraine attack (Michael Assante - SANS ICS Director)

- ▶ Planning
 - ▶ Malware installed - blinded dispatchers
 - ▶ Denial of service to phone system - blocked customer calls
 - ▶ Cause unknown - undesirable state changes to distribution
- ▶ Coordination - multiple utilities attacked
- ▶ Malware used - definite cyber attack
- ▶ Possible direct remote access (unconfirmed)
- ▶ Wiped SCADA servers - to delay restoration

What Western sees monthly - including hits from within US



Removing the US hits



| | |
|---------------|--------|
| South-Korea | 10,708 |
| UnitedKingdom | 10,522 |
| Japan | 10,486 |
| Vietnam | 8,197 |
| Netherlands | 7,013 |
| Ireland | 6,371 |
| France | 5,370 |
| India | 5,014 |
| Poland | 4,275 |
| Kuwait | 3,897 |
| Ecuador | 3,733 |
| Mexico | 3,553 |
| Brazil | 3,363 |
| Italy | 2,866 |
| Ukraine | 2,803 |

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 2012-2014



Insider Threat



- ▶ Angry, frustrated, resentful employees
- ▶ Overly helpful office person
- ▶ Not the sharpest crayon in the box.....
- ▶ IT Staff that is too busy



Risk enhancers

- ▶ Transformer Lead Time
- ▶ Grid Resiliency
- ▶ Lack of rapid Info sharing
- ▶ Sustainable funding
- ▶ Aging Infrastructure
- ▶ Targeted focus
- ▶ Protection varies
- ▶ Dispersed Infrastructure



Cyber Attacks

USA Today article, March 2015— Power Grid

- ▶ Physical and cyber attacks occur 1 in 4 days.
- ▶ 362 plus attacks since 2011
- ▶ Small and large utilities attacked
- ▶ Cited only 14 cyber attacks



Soooooo, what are we actually seeing?

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



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)

2014 Cyber attacks

- ▶ June 2014 - reported by ICS-CERT - HAVEX Trojan-
 - ▶ ICS focused
 - ▶ Multi vector
 - ▶ Phishing e-mails
 - ▶ Redirects to compromised web sites
 - ▶ Watering hole through Trojanized update installers - 3 vendors
 - ▶ Allowed access to networks
 - ▶ Enumerates connected resources
 - ▶ Maps the servers
 - ▶ Denial of service possible



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 Televant



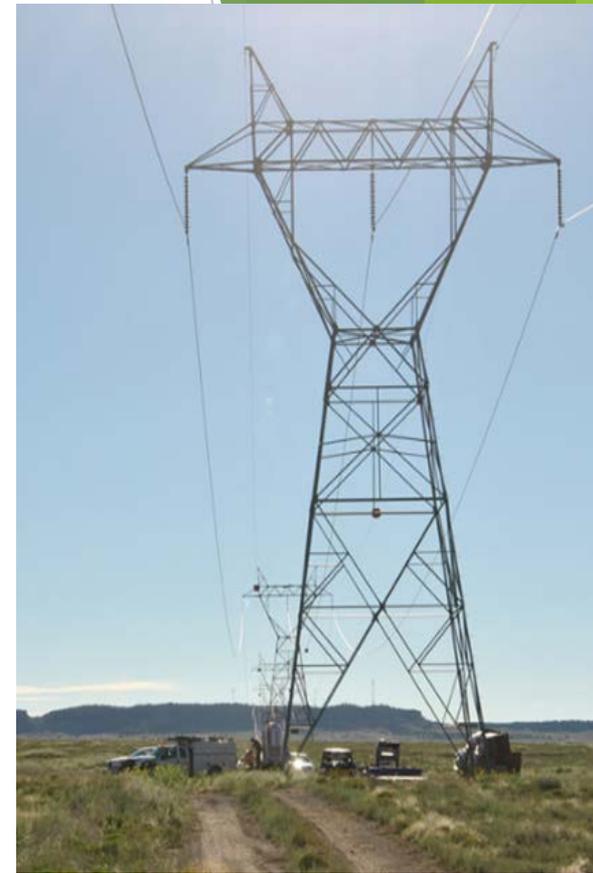
2014 Cyber Attacks

September: Shellshock/Bashdoor

- ▶ Internet facing
- ▶ Attacker can gain control over system
- ▶ Distributed Denial of Service
- ▶ Vulnerability scanning
- ▶ Millions of unpatched servers at risk

October: Black Energy (published by Kaspersky Lab)

- ▶ Converted crimeware tool
- ▶ 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.



2014 Cyber Attacks

December: Sony hacked by North Korea **on US Soil**

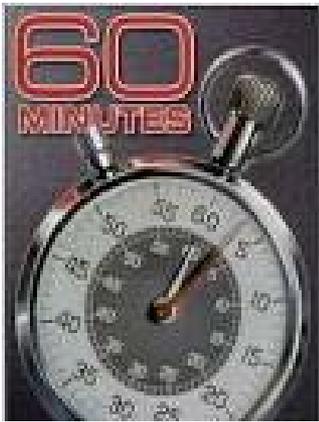
- ▶ Destructive malware deployed
- ▶ Destroyed systems
- ▶ Stole employee Personally Identifiable Information (PII)
- ▶ Stole proprietary information
- ▶ FBI called within hours



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.





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

*“So ... what’s a girl
(or guy) to do?”*



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
- ▶ IT/OT partnership at minimum



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

- ▶ SANS Top 20
- ▶ Vendor Management
- ▶ Apply patches
- ▶ Continuous monitoring
- ▶ Complete a vulnerability assessment and address
- ▶ Intrusion Detection System
- ▶ Intrusion Prevention System



Information Sharing is Critical!

- ▶ Secure, confidential, rapid
- ▶ Actionable
- ▶ Indemnify
- ▶ Cyber happens in milliseconds and is not regional



Governmental Partnerships

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



Information is Power

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



It isn't a question of "If"

Questions

Dawn Roth Lindell
Lindell@wapa.gov

