Mid-West Electric Consumers Association

Presented to: Water & Power Planning Committee
April 7, 2016
Discussion topics

• Western Enterprise Risk overview
• Risk / Cost driver discussion
  – Cybersecurity breach
  – Physical security breach
  – Human capital retention
• Sustainable funding – Unobligated balances
  – Western-wide overview
  – Pick-Sloan Purchase Power & Wheeling (PPW)
Enterprise Risk Overview
Understanding critical risks

Today we will discuss
- Cybersecurity
- Physical security
- Related human capital topics
- Sustainable funding

Inter-related when it comes to cost and risk acceptance

Develop context and common understanding for future discussions
Risk and costs

• Traditional definition is that:
  – Risk = Threats x Vulnerabilities x Impact

• An additional part of the equation:
  \[
  \text{Risk} = \frac{\text{Threats} \times \text{Vulnerabilities} \times \text{Impact}}{\text{Cost}}
  \]
Cybersecurity Breach

At Risk: Increasing Cyber Threats in the Electric Sector/Western response

Dawn Roth Lindell
Cyber attacks: Capability vs. Intent

- The Chinese
- The former USSR nations
- US environmental extremists & anti-government
- Friendly nations
- ISIL
- And then came the December 23, 2015 Ukraine attack
Ukraine Attack, December 23, 2015
An Analysis
by Michael Assante – SANS ICS Director

• Planning
  – Malware installed – blinded dispatchers
  – Denial of service to phone system – blocked customer calls
  – VPN in – undesirable state changes to distribution
  – Wiped SCADA servers – to delay restoration

• Coordination – multiple utilities attacked
• Malware used – definite cyber attack
• Direct remote access
What Western sees monthly: Including hits from within US
Removing the US hits

South-Korea 10,708
United Kingdom 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. They can now have physical impact in the real world.”
  — Steve Durbin, Managing Director, Information Security Forum

• Western Area Power Administration
  – 37 physical attacks in 2014
    • Thefts
    • Reconnaissance
  – 650% increase in cyber incidents 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
Cyber Attacks

Power Grid USA Today article: March 2015

- Physical and cyber attacks occur 1 in 4 days.
- 362+ attacks since 2011
- Small and large utilities attacked
- Cited only 14 cyber attacks
So, what are we actually seeing?

A year of key Cyber Attacks: 2014:

January: Unnamed public utility control system hacked
- Internet facing
- Weak password/brute force susceptible

April: Heartbleed
- Half a million (17%) of Internet's secure web servers believed attack vulnerable
- Allow theft
  - Servers' private keys
  - User session cookies and passwords
- Western:
  - 67 vulnerabilities identified and corrected
2014 Cyber Attacks /Vulnerabilities

• **May:** Five Chinese nationals indicted
  – Computer hacking and economic espionage
  – Targets included Westinghouse Electric

• **June:** 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, maps servers
2014 Cyber Attacks/Vulnerabilities

**June:** Ugly Gorilla hack of Northeastern U.S. Utility
- Exposes cyberwar threat by China
- Stole schematics of pipelines
- Copied security-guard patrol memos
- Cruised channels, keystrokes
  - Potential to cut off a city’s heat, explode a pipeline

**September:**
1. Chinese hackers’ intrusion of Televent
2. Shellshock/Bashdoor
   - Internet facing
   - Attacker can gain control over system
   - Vulnerability scanning
   - Millions of unpatched servers at risk
2014 Cyber attacks/Vulnerabilities

October: Black Energy
- Published by Kaspersky Lab
- Converted crimeware tool
- Cloud based ICS systems at risk
- Can brick systems it infects and skillfully hide from security analysts.

December: Sony hacked by North Korea
- On US Soil!
- Destructive malware deployed
- Stole employee Personally Identifiable Information (PII)
- Stole proprietary information
- FBI called within hours

- Reported March 30 by Nextgov
- Phishing attack vector
- Sever the connection with the network
- Shared drives impacted
- Restore to a state prior to the e-mail receipt
60 Minutes: November 30, 2014

- “97% of all companies are getting breached”
  - Fire Eye CEO Dave DeWalt
- 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
ICS Vulnerabilities

• Study by Positive Research Center, October 2015

• 146,136 ICS components web accessible

• Found 691 vulnerabilities in ICS components
  – 58% high severity
  – 39% medium severity

• By Vendor:
  – Siemens – 124
  – Schneider Electric – 96
  – Advantech – 51
  – GE - 31
Information Sharing is Critical!

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

- Measured response – fiscally responsible
- Implementation of Multi factor authentication costs:

  - Western Area Power Administration $265,000
  - DOE Office of the Chief Information Officer $1,191,692
  - Los Alamos National Lab $777,360
  - Kansas City Plant $705,800
  - Sandia National Laboratories $1,826,682
  - Thomas Jefferson National Accelerator Facility $650,700
Western Response

- Critical Infrastructure Protections v5 – 40,000 hour plus investment
- Network Access Control
- Secure Enclave Systems Control – substations
  - Avoid the spend of $6.5 million over 5 years – Western wide solution
- Eleven required presidential directives
  - Multi factor authentication for administrative and standard accounts
  - Anti –Phishing campaign
Western Response

• 2016 – full inventory of field equipment and supporting technology
  – Every region – all substations
  – Will develop a plan to replace technology

• Supply chain is crucial
  – vendor user groups
  – industry influence on vendor development

• Cyber security training – IT Professionals

• Patching and upgrades MUST stay current
Western Response

• Industry sharing
  – Western Area Power Industry Sharing Pilot

• DOE support
  – CRISP/CPP monitoring
    • Free to Western
  – Negotiated licenses
    • Microsoft cost reduced by nearly 90%
    • DOE wide security tools – purchased by DOE HQ CIO
  – Integrated Joint Cyber Communications Center
Major Cyber Security Expenses by Year

- FY 11- Program Costs: $130,000
- FY 12- NSOC Implementation: $365,791
- FY 13- NSOC Maintenance: $314,095
- FY 14
  - NSOC Maintenance: $486,012
  - Encase: $113,746
- FY 15
  - SESC Implementation: $1.8 million
  - NSOC Maintenance: $511,543
  - Forward Anti-Phish and Training: $30K/Yr
Major Cyber Security Expenses by Year

• FY 16
  – SESC/NSOC Maintenance: $552,640
  – Data Leakage Prevention: $470,000
  – NAC: $350,000 (could be FY 17)

• FY 17
  – NSOC Life Cycle Refresh: $500,000
  – SESC Maintenance: $275,000
  – Begin replacement of old field equipment: $ unknown
  – Sandbox environment: $ unknown

• FY 18  NSOC/ SESC Maintenance: $560,000
## Cyber Security Cost Drivers

### FY 2011 - FY 2017 Costs

<table>
<thead>
<tr>
<th>Year</th>
<th>FTE Labor (Thousands)</th>
<th>Contractor Svcs (Thousands)</th>
<th>Material/Licenses/Services (Thousands)</th>
</tr>
</thead>
<tbody>
<tr>
<td>FY 2011</td>
<td>$443</td>
<td>$300</td>
<td>$162</td>
</tr>
<tr>
<td>FY 2012</td>
<td>$443</td>
<td>$300</td>
<td>$477</td>
</tr>
<tr>
<td>FY 2013</td>
<td>$738</td>
<td>$600</td>
<td>$300</td>
</tr>
<tr>
<td>FY 2014</td>
<td>$738</td>
<td>$600</td>
<td>$528</td>
</tr>
<tr>
<td>FY 2015</td>
<td>$1,475</td>
<td>$600</td>
<td>$1,862</td>
</tr>
<tr>
<td>FY 2016</td>
<td>$1,475</td>
<td>$750</td>
<td>$1,667</td>
</tr>
<tr>
<td>FY 2017</td>
<td>$1,475</td>
<td>$750</td>
<td>$1,217</td>
</tr>
</tbody>
</table>

*Reflects $1.373M CIP V5 Implementation Costs
**Reflects estimated $600K Data Loss Prevention Implementation
FY 2016/FY 2017 also reflect increased carrying costs of the CIP V5 Implementation
IT Cost Savings/Avoidance

FY 2015 Total Savings $5.8M

- $1,025: Purchase Consolidation
- $633: Travel for Training
- $488: Hardware
- $471: Systems
- $177: Personnel
- $3,020: Processes/Work Efficiencies
Projects delayed

- 205 projects requested initially for 2016
- 32 are legally mandatory
- Key projects delayed:
  - Improved network segmentation (security)
  - Improved Network Access Control (security)
  - Expansion of network for IP meters
  - Replace SONET infrastructure – past end of life
  - Provide IP management for IP radios (security)
  - Upgrade VTC (cost savings)
  - Network lifecycle replacements
  - Plus 100 others
IT Evolution –
Physical Security Breach
Managing Physical Security Risk

Risk due to malicious actor is INCREASING!

- Societal disruption due to increased dependencies
- Costs to repair damaged infrastructure
- Costs due to service outages
- Long term service disruptions
- Harm to employees
- Harm to public

- Numbers of breaches
- Severity and sophistication of breaches (Mecalf)
- Insider threats
- Discontent among domestic actors
- Foreign terrorists

- Aging protection infrastructure
- Vulnerability to new threats
- (UAV, Coordinated attacks)
- Availability of sensitive information
- Long lead time equipment replacement

- Societal disruption due to increased dependencies
- Costs to repair damaged infrastructure
- Costs due to service outages
- Long term service disruptions
- Harm to employees
- Harm to public

- Numbers of breaches
- Severity and sophistication of breaches (Mecalf)
- Insider threats
- Discontent among domestic actors
- Foreign terrorists

- Aging protection infrastructure
- Vulnerability to new threats
- (UAV, Coordinated attacks)
- Availability of sensitive information
- Long lead time equipment replacement
National Breaches

- **Vandalism:** 1 incident
- **Surveillance:** 10 incidents
- **Intrusion:** 6 incidents
- **Sabotage:** 8 incidents
- **Theft:** 4 incidents
Inspector General Audits
Findings Through the Years

• 2003:
  – Risk assessments inadequate

• 2010:
  – Incomplete required risk assessments, security measure performance testing, and implementation of recommended security enhancements

• 2013:
  – Formalized Office of Security and Emergency Management
  – Consolidated Western’s security programs

• 2014:
  – Updated Risk Management process
  – Developed All Hazard risk assessment

• 2016:
  – Progress noted
  – New recommendations; Regions working through lists
Western’s response

• Agile process; culture of compliance
• Making strides in all areas
• Consistent high marks in NERC, WECC
• Fundamental Security Commitment
Risk Assessments and Reporting

• NERC CIP 14 – Risk to Bulk Electric System
  – 10 Western CIP 14 sites
  – CIP 14 sites assigned highest baseline Facility Security Levels
  – Reassess every 2.5 years

• Current status
  – Validation of study work complete
  – Development and verification of mitigation plans in progress
  – Average estimated mitigation cost estimate per site $677k
    • Highest site - $2.161M (located in UGP)
    • Lowest site - $64k (located in SNR)

• Non-CIP 14 sites (330+)
  – Baseline assessments underway and to be completed by 2019
  – Reassess every 5 years
WESTERN AREA POWER ADMINISTRATION

Human Capital Challenges
# Human Capital SWOT Analysis

<table>
<thead>
<tr>
<th>Internal</th>
<th><strong>Strengths</strong></th>
<th><strong>Weaknesses</strong></th>
</tr>
</thead>
</table>
| **Enablers** | • Industry leading technical experts  
               • Western institutional knowledge  
               • Passion and commitment to Western’s mission and customers | • Aging workforce – mission critical positions  
               • Retirement eligibility growing rapidly  
               • Managerial development |

<table>
<thead>
<tr>
<th>External</th>
<th><strong>Opportunities</strong></th>
<th><strong>Threats</strong></th>
</tr>
</thead>
</table>
| **Challenges** | • Strengthen workforce planning and management  
                 • Improve leadership development  
                 • Improve knowledge management | • Extensive competition for engineers, IT specialists, and experienced senior managers  
                 • Younger workforce mobility |
Retirement eligible projections

- 2015 & Prior*: 13.2%
- 2016: 17.8%
- 2017: 21.7%
- 2018: 25.2%
Engineering special pay rate initiative

• Joint study with other PMAs
• Aimed at mitigating risks such as:
  – PMAs compensate new graduates 11% - 19% lower than industry
  – PMAs compensate existing engineers 6% - 67% lower than industry
  – 46% of industry engineers estimate to retire within the next 5 – 10 years
• Presented proposed adjustment through DOE
• Annual (FY17-20) impact = $4.3M - $4.7M
Other potential salary impacts

- General schedule locality adjustments and cost of living increases
- Wage board salary increases
- Administratively determined salary increases
- Senior executive salary adjustments
Sustainable Funding

Unobligated Balances Overview
Where We Are Now: Funding
Unobligated Balances Strategy

• Sustainable funding tool in support of Western’s mission
  – Sound fiscal management
  – Continue operations during emergency situations
  – Mitigates risk during continuing resolutions or lapses in appropriations

• GAO Audit: Committed to Congress to finalize and implement unobligated balances strategy
How are unobligated balances created?

• Difference between amounts budgeted and executed

• Some illustrative examples:
  – Mitigate risk such as PP&W
  – Construction project delays in execution years
  – Employee pay raises budgeted but not enacted
  – Revenue exceeds power repayment study estimate:
    • Better than average water year
    • Selling power high to cover contract commitment purchases later in the day
FY15 Position vs. Current strategy

FYE 15 Unobligated by Purpose
Total $793 (in Millions)

- Other (Reimb, Misc revolving, TIP) $104
- PPW $183
- Capital $371
- Annual $135

Unobligated Strategy by Purpose
Total $817 (in Millions)

- Other (Reimb, Misc revolving, TIP) $103
- PPW Minimum $393
- Capital Minimum $250
- Annual Minimum $71
Discussion items

- Potential strategies
- Relationship to rates
- Repayment versus return
Sustainable Funding

Pick-Sloan Purchase Power & Wheeling (PPW)
Background

• PPW initiative identifies a Western-wide minimum threshold for PPW
• Each region collaborating with it’s customers to identify project needs
• Introduced at Feb. 2016 Water & Power Planning Committee meeting
• Presented analysis at March 2016 Board meeting
• Today serves as additional collaboration
Purchased Power - Firming - P-SMBP

Purchases vs Energy

Drought
2001-10 Drought $ on Net Energy Purchased* (Pick-Sloan)

($000)

Year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010

- Cumulative Additional Revenues from Firm Rate Increases
- Mainstem Dec Storage
- Mainstem runoff

* Total energy purchased less non-
Cumulative P.Power $ over a 3-Yr Sliding Window (Pick-Sloan)