Enterprise Risk Overview
Risk, Security and Staff

July 11, 2016
Sierra Nevada All-Customer Meeting
Folsom, California
Introduction and Purpose
Mark A. Gabriel | Administrator and CEO
Understanding critical risks

- Today we will discuss
  - Cybersecurity
  - Physical security
  - Human capital

- 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:
  - Risk = Threats x Vulnerabilities x Impact
  - Cost
Cyber Security
Dawn Roth Lindell | Senior VP and CIO
Cyber attacks: capability vs. intent

• China
• The former USSR nations
• U.S. environmental extremists & anti-government
• Friendly nations
• ISIL
• Dec. 23, 2015 Ukraine attack
Ukraine Attack: an analysis

Dec. 23, 2015

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 WAPA sees monthly:
Including hits from within U.S.
Removing the U.S. hits

### Other Hits

<table>
<thead>
<tr>
<th>Country</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>South-Korea</td>
<td>10,708</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>10,522</td>
</tr>
<tr>
<td>Japan</td>
<td>10,486</td>
</tr>
<tr>
<td>Vietnam</td>
<td>8,197</td>
</tr>
<tr>
<td>Netherlands</td>
<td>7,013</td>
</tr>
<tr>
<td>Ireland</td>
<td>6,371</td>
</tr>
<tr>
<td>France</td>
<td>5,370</td>
</tr>
<tr>
<td>India</td>
<td>5,014</td>
</tr>
<tr>
<td>Poland</td>
<td>4,275</td>
</tr>
<tr>
<td>Kuwait</td>
<td>3,897</td>
</tr>
<tr>
<td>Ecuador</td>
<td>3,733</td>
</tr>
<tr>
<td>Mexico</td>
<td>3,553</td>
</tr>
<tr>
<td>Brazil</td>
<td>3,363</td>
</tr>
<tr>
<td>Italy</td>
<td>2,866</td>
</tr>
<tr>
<td>Ukraine</td>
<td>2,803</td>
</tr>
</tbody>
</table>

---

**Top 5 Blocks by Country -- Excluding the Untied States**

- China: 13,140
- Canada: 19,579
- Germany: 20,666
- South Africa: 24,734
- Russia: 122,038
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

• WAPA
  ▪ 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
A year of key cyber attacks: 2014

**January:** A 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
- WAPA:
  - 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

Sierra Nevada All-Customer Meeting
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 networks, viewed keystrokes
  - Potential to cut off a city’s heat, explode a pipeline

**September:**
1. Chinese Government 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
- 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 U.S. soil!
- Destructive malware deployed
- Stole employee Personally Identifiable Information
- Stole proprietary information
- FBI called within hours
Ransomware fed agencies attacked

March 2016

- Reported March 30 by Nextgov
- 321 total agencies attacked
- Phishing attack vector
- Sever the connection with the network
- Shared drives impacted
- Restore to a state prior to the email receipt
60 Minutes
Nov. 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 username and password from vendor
  ▪ Installed malware to steal credit card info
ICS vulnerabilities

• Study by Positive Research Center, Oct. 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

Leveraging Relationships
WAPA 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
WAPA response

• Critical Infrastructure Protections v5 – 40,000 hours plus investment

• Network Access Control

• Secure Enclave Systems Control – substations
  ▪ Avoid spending $6.5 million over 5 years – WAPA-wide solution

• 11 required presidential directives
  ▪ Multi-factor authentication for administrative and standard accounts
  ▪ Anti-phishing campaign
WAPA 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
WAPA response

• Industry sharing
  ▪ WAPA Industry Sharing Pilot

• DOE support
  • CRISP/CPP monitoring
    ▪ Free to WAPA
  • 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 fiscal 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-phishing and training: $30,000/year
Major cyber security expenses

• 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

The diagram and table below illustrate the trend in cost drivers from FY 2011 to FY 2017.

### Cost Drivers Breakdown

<table>
<thead>
<tr>
<th>Year</th>
<th>FTE Labor</th>
<th>Contractor Svc</th>
<th>Material/Licenses/Services</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>

### Bar Chart

The bar chart visualizes the cost drivers across different fiscal years.
IT cost savings/avoidance

FY 2015 Total Savings $5.8M

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

IT 5 years ago

IT Today
Physical Security
Anthony Montoya | Executive VP and COO
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

Physical security risk

- Number of breaches
- Severity and sophistication of breaches (Metcalf)
- 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

RISK

Threat

Consequence

Vulnerability
National breaches

- Vandalism: 1 incident
- Surveillance: 10 incidents
- Intrusion: 6 incidents
- Sabotage: 8 incidents
- Theft: 4 incidents

Sierra Nevada All-Customer Meeting
Inspector general audits

- 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 WAPA’s security programs
    - 2014
      - Updated Risk Management process
      - Developed All-Hazard Risk Assessment

- 2016
  - Progress noted
  - New recommendations; regions working through lists
WAPA’s response

- Agile process and culture of compliance
- Making strides in all areas
- Consistent high marks in NERC, WECC, MRO
- Fundamental security commitment
Risk assessments

• NERC CIP 14 – risk to bulk electric system
  ▪ 10 WAPA CIP 14 sites
  ▪ CIP 14 sites assigned highest baseline facility security levels
  ▪ Reassess ever 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 SN)

• Non-CIP 14 sites (330+)
  ▪ Baseline assessments underway and to be completed by 2019
  ▪ Reassess every five years
Risk assessments

Figure 9.2 - Levels of Protection and Risk Graph
Security Evolution

Security 3 years ago

UGP
- Safety
- Risk Management
- Physical Security
- Personnel Security
- Emergency Management

RM
- Safety
- Risk Management
- Physical Security
- Personnel Security
- Emergency Management

SN
- Safety
- Risk Management
- Physical Security
- Personnel Security
- Emergency Management

DSW
- Safety
- Risk Management
- Physical Security
- Personnel Security
- Emergency Management

Security Today

- Risk Management
- Physical Security
- Personnel Security
- Emergency Management
Raptor X

• Flexible platform for intelligence collection, monitoring, and analysis
• Geo-data interfaced
Raptor- X

• Developed by Department of Energy STL
• Pilot in an electric utility environment at SN
Human Capital
Anthony Montoya | Executive VP and COO
# Human capital SWOT analysis

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

<table>
<thead>
<tr>
<th>External</th>
<th>Opportunities</th>
<th>Threats</th>
</tr>
</thead>
</table>
| • 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

<table>
<thead>
<tr>
<th>Year</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015 &amp; Prior*</td>
<td>13.2%</td>
</tr>
<tr>
<td>2016</td>
<td>17.8%</td>
</tr>
<tr>
<td>2017</td>
<td>21.7%</td>
</tr>
<tr>
<td>2018</td>
<td>25.2%</td>
</tr>
</tbody>
</table>
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 (FY 17-20) 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
Linda Kimberling | Senior VP and CFO
Where we are now: funding
How we get unobligated balances

• 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
Unobligated balances strategy

• Sustainable funding tool in support of WAPA’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
Moving strategy forward

FYE 15 Unobligated Balance
By purpose: $793 (in Millions)

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

FYE 16 Estimated Unobligated Balance
By purpose: $817 (in Millions)

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

Sierra Nevada All-Customer Meeting
Discussion and Comments
Subhash Paluru | Senior VP and SN Regional Manager
Committed to transparency

• Lowest possible rates consistent with sound business principles
• Critical to focus on the big issues we are all facing
• Need customer support to meet your changing needs
• Customer engagement is critical
• The Source: www.wapa.gov
What is next?

• Collecting your thoughts
  ▪ Keeping dialogue open
  ▪ Customer meetings
Thank you