WANG & ASSOCIATES
Security & Compliance Consulting

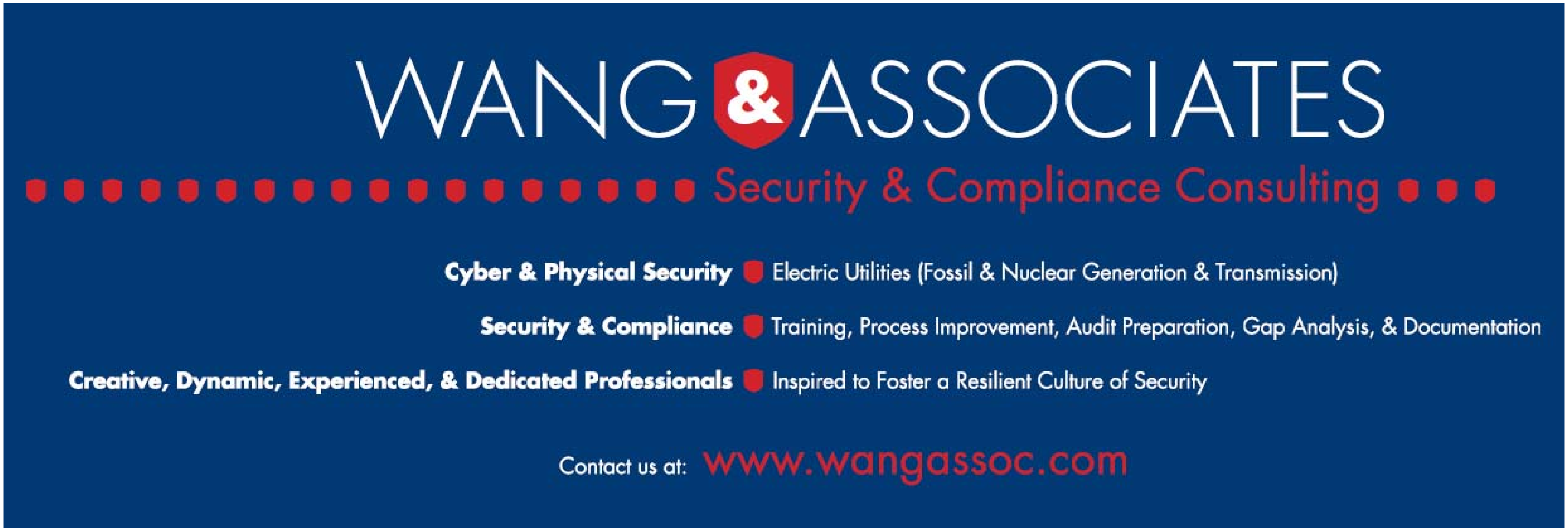
# Purpose-Built, Industrial Control System:

## Collaborative Effort to Design, Build and Document a Security Appliance Beyond Regulatory Compliance

Anna M Wang
Principal Consultant
Wang & Associates

January 15, 2014
2nd Annual Utility Cyber Security Conference

# Who are Wang & Associates?



WANG & ASSOCIATES

Security & Compliance Consulting

**Cyber & Physical Security** Electric Utilities (Fossil & Nuclear Generation & Transmission)

**Security & Compliance** Training, Process Improvement, Audit Preparation, Gap Analysis, & Documentation

**Creative, Dynamic, Experienced, & Dedicated Professionals** Inspired to Foster a Resilient Culture of Security

Contact us at: www.wangassoc.com

# Summary of Case Study

- Describes the benefits of a collaborative effort among power utilities, security professionals and an industrial control system vendor to design a **purpose-built security appliance—defense-in-depth**
- Securing of digital systems and communication systems from insider threats associated with cyber security intrusion, **includes supply chain hardening**
- Assesses sophisticated logging and patch management configuration to secure plant control systems **beyond compliance**, with AURORA Mitigation, NERC CIP and NEI 08-09 Revision 6 regulatory requirements
- Strengthens the security posture of power utilities through collaborative documentation efforts, procurement and factory acceptance testing**—defense-in-breadth**
- Reinforces reliable operations of power plants while reducing the cost of labor-intensive processes**—making cyber security investment resilient**

# Attack on a California Power Station

- The April 16 attack saw as many as two gunmen storm the PG&E Metcalf substation after severing phone service and fire several dozen rounds at transformers.

- “*Not amateurs taking potshots… this was a dress rehearsal” — possibly for large-scale attacks on power stations”* according to a PG&E spokesman.

Image source: Surveillance video of substation attack

Source:
[http://www.theblaze.com/stories/2013/12/28/was-mysterious-attack-on-calif-power-station-a-dress-rehearsal-for-much-larger-assault-on-u-s-electrical-grid/](http://www.theblaze.com/stories/2013/12/28/was-mysterious-attack-on-calif-power-station-a-dress-rehearsal-for-much-larger-assault-on-u-s-electrical-grid/)

# Anticipatory Computing

- FortiGate is wirelessly capturing the presence of the unique MAC address on the shopper's smartphone if it is turned on.
  - “Real-time visibility” means the store's wireless security gateway is also being put into use for real-time monitoring of shopper's presence and push marketing to them via Facebook or Twitter.

- IBM predicts a trillion sensors from smart handhelds by 2015.
  - Global networks of High Performance Computing (HPC) can process those trillions of bits of information coming from all those sensors in mere seconds.

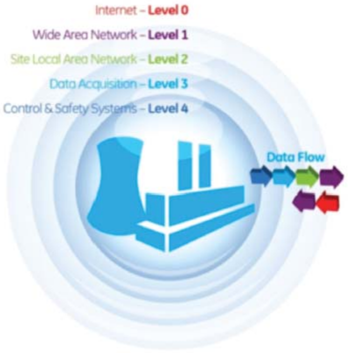
- Social Attack Tsunami: As many as 110 million Target customers impacted
  - Credit and debit card hack over 19 days at the peak of the holiday shopping season, November/December 2013.
  - JPMorgan is replacing 2 million cards after the Target hack.

# A Collaborative Model to Accelerate Solutions

- A collaborative effort among power utilities, Wang & Associates and GE Measurement & Control - design of a **purpose-built cyber security appliance** (SecurityST)**.**
- The purpose-built appliance was based on the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). The ES-C2M2 maturity model provides a mechanism to evaluate, prioritize, and improve cybersecurity capabilities.
- GE engaged power utilities for input based on utilities' developed road maps, strategic initiatives, and risk profiles.
- Wang & Associates consultants assisted these utilities in risk assessments and road map development based on the Cybersecurity Risk Management Process (RMP) Guideline and the 2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity.

# Purpose-Built Security Appliance

- **Defense-in-depth** is an information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions organization. *[Committee on National Security Systems CNSSI 4009]*


Internet – Level 0
Wide Area Network – Level 1
Site Local Area Network – Level 2
Data Acquisition – Level 3
Control & Safety Systems – Level 4
Data Flow

- **Defense-in-breadth** is a planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).

Sources: CNSSI 4009: National Information Assurance (IA) Glossary, April 26, 2010
NIST SP800-39: Managing Information Security Risk Organization, Mission, and Information System View, March 2011

# Cyber Security Standards and Guidelines

**Nuclear Energy Institute Cyber Security Controls 08-09 Rev. 6**

- Cyber security plan for nuclear facilities in North America
- Protection of information flows
- High Assurance of critical digital assets

**International Instrument Users' Association (WIB) Version 2.0**

- Process Control Domain – Security Requirements for Vendors
- Oil and Gas
- Power Generation

**International Society for Automation ISA-99**

- Asset Owners
- System Integrators
- Component Providers
- ANSI accredited ISASecure Certification of PLC, DCS, and SIS

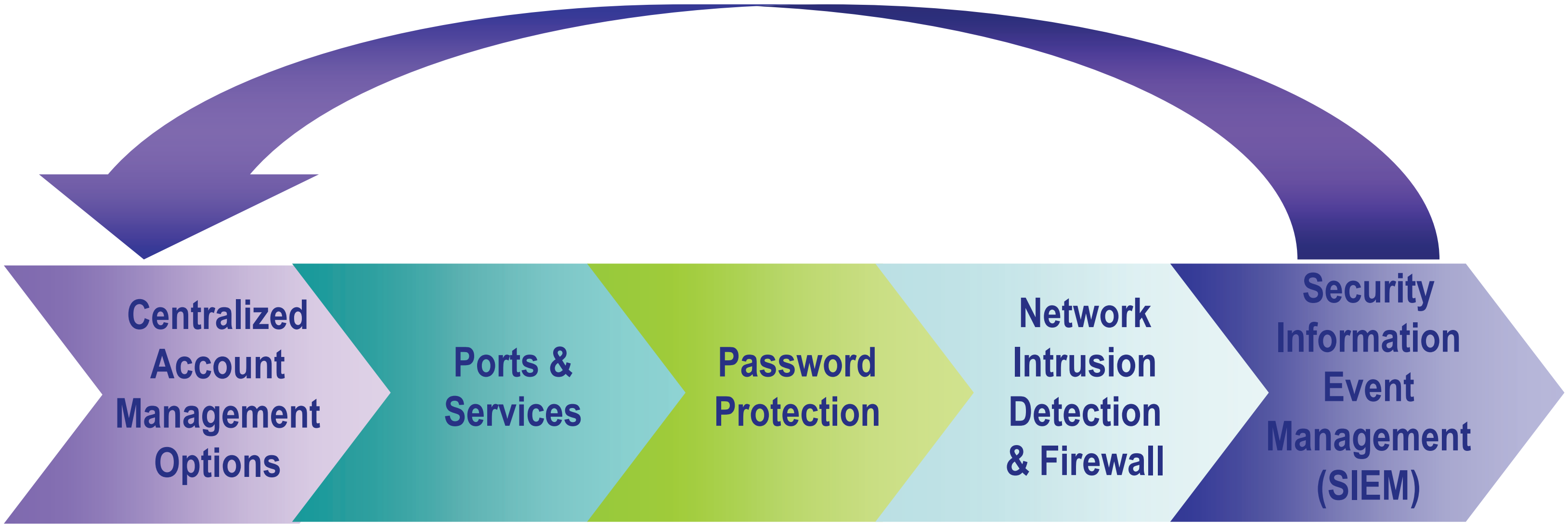
**North American Electric Reliability Corporation CIP Standards V3**

Generator Owners and Operators
Transmission Owners & Operators
Version 3—enforced until Mar. 31, 2016
Version 5—effective April 1, 2016 (except CIP-003-5 R2—April 1, 2017)

# Cyber Security Standards, Guidelines, and Resources

- NEI 13-10, “Cyber Security Control Assessments,” Revision 0, October 2013.
- NERC Security Guideline for the Electricity Sub-sector: Physical Security Response, Approved by CIPC on October 28, 2013.
- Industrial Control System (ICS) Cybersecurity Response to Physical Breaches of Unmanned Critical Infrastructure Sites: a SANS Analyst Whitepaper written by Scott D. Swartz and Michael J. Assante, January 2014.
- Cyber Security Procurement Language for Control Systems, September 2009
- ISO27036-3 (ISO 27036-3) Guidelines for ICT Supply Chain Security
- ISO/IEC 27036-3:2013 Information technology -- Security techniques -- Information security for supplier relationships -- Part 3: Guidelines for information and communication technology supply chain security

# Cyber Security Best Practices



Centralized Account Management Options

- Active Directory
- MS RADIUS Server
- Certificate Authority Server

Ports & Services

- Normal Operation
- Emergency Operation

Password Protection

- Password Strength
- Password Lifetimes
- Reuse Restrictions

Network Intrusion Detection & Firewall

- Host-based Intrusion Detection System (HIDS)
- Detection of Known or Suspicious Network Activity
- Application Whitelisting
- Redundant Firewalls

Security Information Event Management (SIEM)

- Centralized Real-time Display
- Correlates Endpoint Events
- Access Control Review
- Incident Alert & Alarm
- Configuration Management Review
- Compliance Audit Trail

# Supply Chain Hardening

- Establishment of trusted distribution paths
- Validation of vendors including onsite physical security assessment
- Provide physical and cyber security training to third-party supply chain vendors
- Provide detailed training on step-by-step procedures on chain of custody and baseline configuration capture
- Outline requirements for tamper proof products or tamper evident seals on acquired products

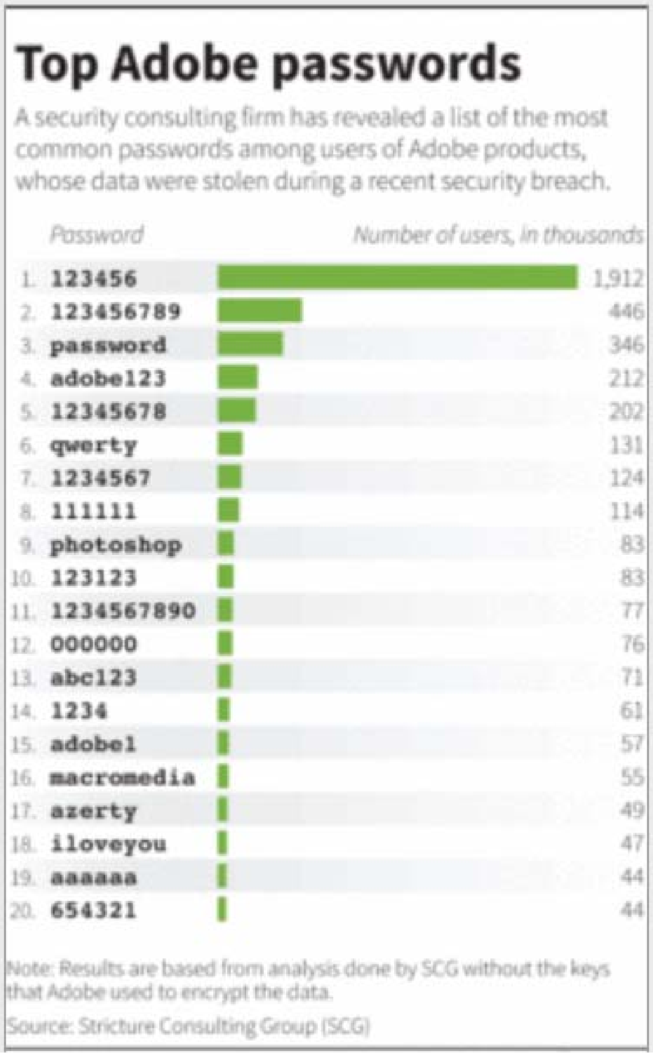
- CAP Security Patch Management Subscription Test Certification and hash comparison tool to ensure the integrity of patch management firmware.

# Windows Password Settings

- **ANIXIS Password Policy Enforcer (PPE)**
  - Windows Password Policy  [NEI 08-09 Rev. 6, D4.3]
    - Minimum Characters - 8
    - Complexity – Enabled
    - Maximum Age – 92 Days
    - Store Using Reversible – Disabled
    - Minimum Age – 1 Day
    - Password History – 24
  - Non-authenticated Human Machine Interactions (NHMI) accounts for SIEM monitoring, patching and anti-virus agents, accounts for service logons, and batch/scheduled processes: [NEI 08-09 Rev. 6, D4.4.2]
    - Minimum Characters – 15
    - *FOUR* of the complexity parameters: lower alpha, upper alpha, numeric, special complexity

# Adobe Password Breach

- **Adobe Breach in Fall 2013**
  - Exposed user IDs, passwords and credit-card information on about 2.9 million customers.
  - The Stricture Group was able to compile a list of the top 100 passwords selected by Adobe users because Adobe chose to use symmetric key encryption over hashing, selecting ECB mode, and using the same key for every password, combined with a large number of known plaintexts password hint.



**Top Adobe passwords**

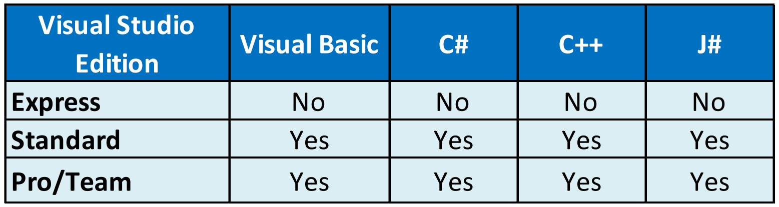
A security consulting firm has revealed a list of the most common passwords among users of Adobe products, whose data were stolen during a recent security breach.

Note: Results are based from analysis done by SCG without the keys that Adobe used to encrypt the data.

Source: Stricture Consulting Group (SCG)

# Close Hardware & Firmware Backdoors

- **Debugger**
  - The GNU Debugger (GDB) allows debugging of programs written in C, C++, Java, and other languages by executing them in a controlled fashion and then printing out their data.
  - GNU Project Debugger (GDB) before 7.5, when .debug_gdb_scripts is defined, automatically loads certain files from the current working directory, which allows local users to gain privileges via crafted files such as Python scripts to obtain information, perform unauthorized modification, or disrupt service (Vulnerability Summary for CVE-2011-4355, last revised on March 6, 2013).
  - Disable debug in Cisco switches because debugging output is assigned high priority in the CPU process, it can render the system unusable.
  - Disable Windows Just-In-Time Debugging

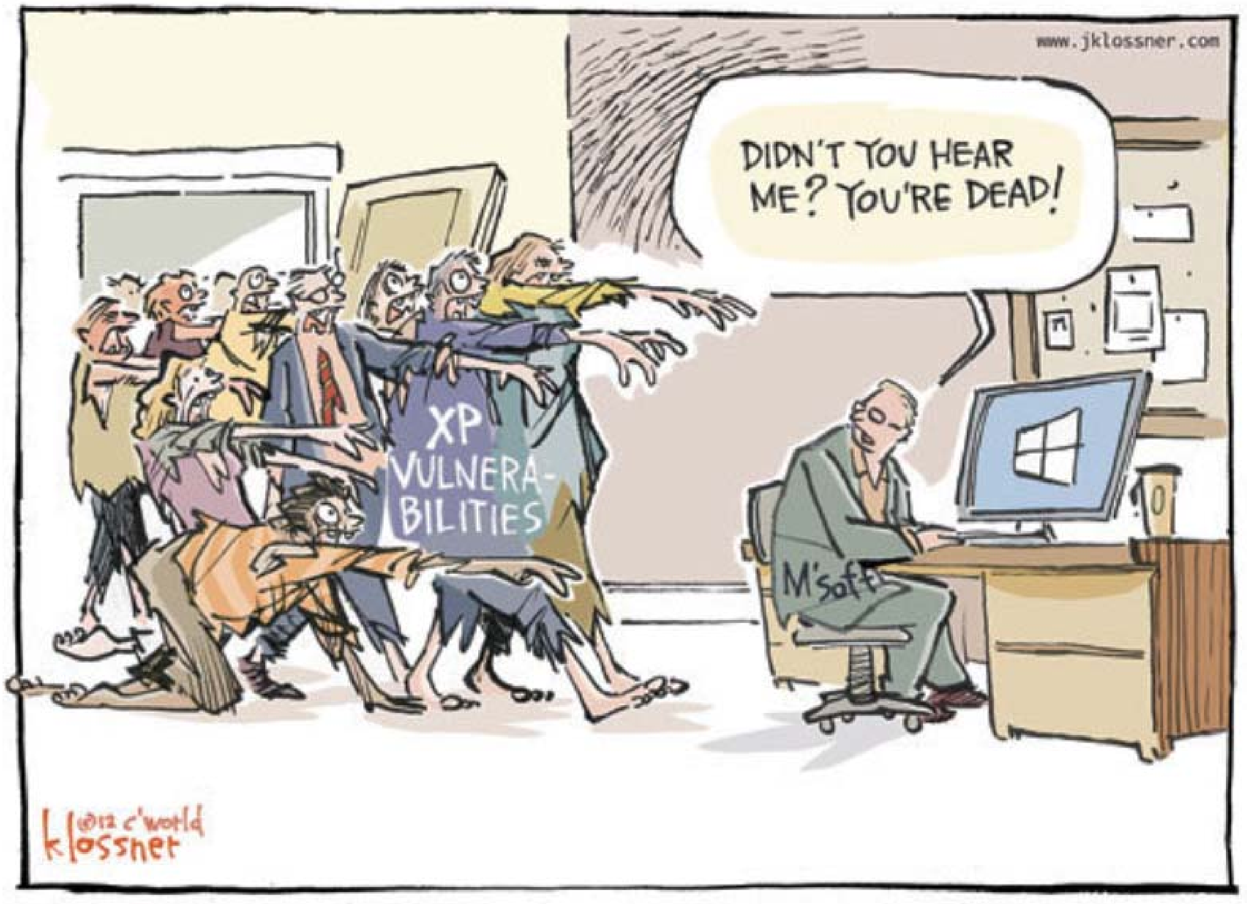


| Visual Studio Edition | Visual Basic | C# | C++ | J# |
|---|---|---|---|---|
| **Express** | No | No | No | No |
| **Standard** | Yes | Yes | Yes | Yes |
| **Pro/Team** | Yes | Yes | Yes | Yes |

# Close Hardware & Firmware Backdoors

- **Hardware Backdoor**
  - An attacker using a debugging tool compliant with IEEE Std. 1149.1, Standard Test Access Port and Boundary Scan Architecture and bound (JTAG) can easily access the processor or the memory-internal information of a device equipped with the port.
  - The NSA's Ironchef product provides access persistence using a hardware implant that provides two-way RF communication by exploiting the motherboard BIOS.
  - GOURMETTROUGH is a user configurable persistence implant for Juniper firewalls which persists across reboots and OS upgrades.
  - Halluxwater is a persistence Back Door implant installed as a boot ROM upgrade on Huawei firewalls.

# Software End of Life Cycle



**Used with permission from John Klossner**

# Portable Devices

- **Portable Devices**
  - Removable devices such as USB “memory sticks” or “flash drives” may carry viruses and malware and cause CDAs to become vulnerable to cyber attacks.
  - On April 29, 2013, the Department of Homeland Security Industrial Control System Cyber Emergency Response Team warned that Stuxnet and other malware take advantage of USB drives to propagate.
  - In October 2012, a computer virus attacked a turbine control system at a U.S. power company when a technician of a third-party contractor unknowingly inserted an infected USB computer drive into the network, keeping a plant off line for three weeks, according to a report posted on the DHS website.
  - Disable autorun as part of system hardening to prevent malicious codes to execute from USB or other portable devices.
  - Always scan USB devices for virus and malware prior to using them.
  - Remember to encrypt and secure sensitive data because portability means that these USB pocket devices can easily be misplaced, infected, or stolen.

# Security Resiliency

- **Spot Audit of Network Logs**
  - Conduct spot audit of network logs to ensure accountability
  - Verizon investigated a malware incident which an open and active VPN connection originating from China was used.
    - A client's employee who outsourced his job to China, the developer in China logged in as the employee using his credentials while the employee sat in his office  watching cat videos, reading stories on Reddit and spending time on eBay, Facebook and LinkedIn.

  - Traffic Gist is a network traffic statistics collection tool. Gist can collect statistics about live traffic and do postmortem packet capture analysis for DNS and DHCP forensic investigation.

# Security Resiliency

- **Change Monitoring**
  - Monitoring of changes to configuration files, registry, active directories, databases, physical and virtual events, across the entire control network.
  - Sysadmins can search this data to investigate service problems and identify the root cause change events caused by unauthorized and authorized changes.
  - Option to turn searches into alerts to proactively monitor and notify them of unauthorized changes, high impact changes, changes outside of change windows, and changes to critical hosts.
  - Facilitate forensic investigation of cyber incidents by reviewing the impact of changes, by searching for activity on a given host or application before and after changes.
  - Resolve performance issues faster by correlating infrastructure problems with service availability and response time problems.

# Security Resiliency

- Breaking down silos among utilities, vendors, and regulatory agencies. Cyber Security Information Sharing, Section 4 of Executive Order -- Improving Critical Infrastructure Cybersecurity, February 12, 2013
- NERC Reliability Assurance Initiative program "is the Electric Reliability Organization's strategic initiative to transform the current compliance and enforcement program into one that is forward looking, focuses on high reliability risk areas and reduces the administrative burden on registered entities."

- Knowledge and prevention is the key to safe guard security. We need to invest in the "intangibles" to improve defense-in-breadth for resiliency and build the security knowledge assets of this nation.
- *"Not everything that counts can be counted, and not everything that can be counted counts." "We can't solve problems by using the same kind of thinking we used when we created them" ~ Albert Einstein ~*

# Question & Discussion

Send questions and comments to

amwang@wangassoc.com
tzcole@wangasso.com

Thank you!