WANG & ASSOCIATES
Security & Compliance Consulting

Maturation of a Cyber Security Incident Prevention and Compliance Program

Utilities & Energy Compliance & Ethics Conference
February 25, 2013
Houston, Texas

Anna Wang
Principal Consultant

WANG & ASSOCIATES
Security & Compliance Consulting

Imminent "Cyber 9/11"

- Speaking at the Woodrow Wilson International Center for Scholars on January 24, 2013, Janet Napolitano, US Secretary for Homeland Secretary, said a "cyber 9/11" could happen "imminently" and that critical infrastructure - including water, electricity and gas - was very vulnerable to such a strike.

  Source: http://www.wilsoncenter.org/event/cyber-to-immigration-terrorism-to-disasters-securing-america-the-next-administration

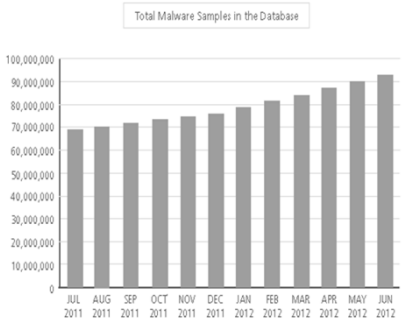
- During the Face*the*Nation discussion on February 10, 2013, Mike Rogers, chair of the US House Intelligence Committee, told CBS that the US government has essentially "*set up lawn chairs, told the burglars where the silver is ... and opened the case of beer and watched them do it*".

  Source: http://www.cbsnews.com/video/watch/?id=50140732n

WANG & ASSOCIATES
Security & Compliance Consulting

Imminent "Cyber 9/11"

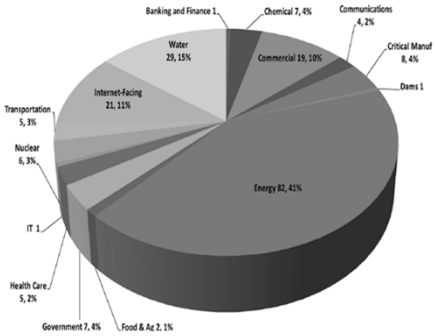
- US House Intelligence Committee estimates 95% of private sector networks are vulnerable, and most have been penetrated, causing an estimated loss of up to $400 billion every year. Source: http://www.cbsnews.com/video/watch/?id=50140732n
- McAfee reported in its Threat Report that malware was closing in on a rate of nearly 100,000 unique samples per day in second quarter 2012; possibly the first 10 million-sample quarter in 3rd Quarter 2012.



WANG & ASSOCIATES
Security & Compliance Consulting

Imminent "Cyber 9/11"

- DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) responded to 198 cyber incidents reported by energy companies, public water districts and other infrastructure facilities in the fiscal year ending Sept. 30, 2012.



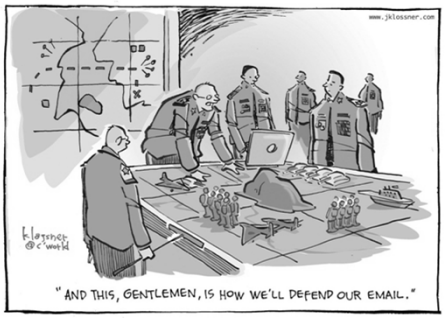
Attacks against the energy sector represented 41% of the total number of incidents

Source: http://ics-cert.us-cert.gov/pdf/ICS-CERT_Monthly_Monitor_Oct-Dec2012.pdf

WANG & ASSOCIATES Security & Compliance Consulting

Imminent "Cyber 9/11"

- ICS-CERT assisted 23 oil and natural gas entities after they were attacked by a targeted spear-phishing campaign - when E-mails with malicious content are specifically targeted at their employees.
- Analysis of the targeted systems indicated that information pertaining to the ICS/SCADA environment, including data that could facilitate remote unauthorized operations, was exfiltrated.



Used with permission from John Klossner, February 2012

WANG & ASSOCIATES Security & Compliance Consulting

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 and Operators Version 4—Mar. 31, 2013 Version 5—TBD

WANG & ASSOCIATES Security & Compliance Consulting

Regulatory Complexity

- The proposed European Commission's Directive on Network and Information Security, released on February 7, 2013, mandates companies to notify a national authority whenever their services have been disrupted or data privacy breached, including cases of human error, natural disasters or extreme weather, as well as cyber attacks. The Directive must be reviewed by the European Parliament and the leaders of the EU's 27 national governments before becoming law.

  Source: http://europa.eu/rapid/press-release_IP-13-94_en.htm

- After the defeat of the S. 2105, the Cybersecurity Act of 2012, the President issued the Executive Order "**Improving Critical Infrastructure Cybersecurity**" on February 12, 2013.

WANG & ASSOCIATES Security & Compliance Consulting

Regulatory Complexity

- The Executive Order addresses three areas:
  - Voluntary information sharing
  - Creating a flexible risk-based framework of core practices based on existing standards
  - Incorporating privacy protections.

- To develop the Framework, NIST will use a Request for Information (RFI) and ongoing stakeholder engagement to:
  - identify existing cybersecurity standards, guidelines, frameworks, and best practices that are applicable to increase the security of critical infrastructure sectors and other interested entities
  - specify high-priority gaps for which new or revised standards are needed
  - collaboratively develop action plans by which these gaps can be addressed.

WANG & ASSOCIATES
Security & Compliance Consulting

Regulatory Complexity

- On October 13, 2011, the U.S. Securities and Exchange Commission (SEC) issued disclosure guidance related to cyber security risks and costs that may have far-reaching impacts on electric utilities. For those electric utilities already subject to NERC cyber security requirements, this guidance suggests the need for increased scrutiny of compliance costs and harms resulting from cyber incidents and potential cyber incidents to evaluate appropriate disclosure.
- With the pending increase in the number of assets covered by the Version 5 CIP Reliability Standards, which were approved by the NERC Board of Trustees on November 26, 2012, the costs of compliance are likely to significantly increase across the electric utilities industry, affecting a wide variety of SEC registrants subject to FERC's reliability jurisdiction

WANG & ASSOCIATES
Security & Compliance Consulting

Get Ahead of the Compliance Curve

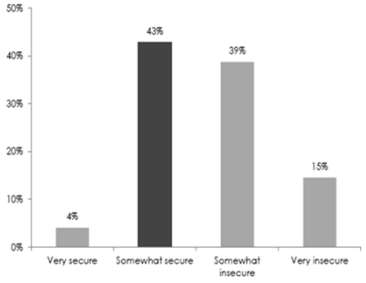
- During the Cyber Security and the Grid Senate Hearing on July 17, 2012, Mr. Gerry W Cauley, North American Electric Reliability Corporation (NERC) President and Chief Executive Officer testified that compliance with NERC CIP standards is not enough; *"is an important threshold for properly securing the bulk electric system. However, no single security asset, technique, procedure, or standard—even if strictly followed—will protect an entity from all potential cyber threats. The cybersecurity threat environment is constantly changing and our defenses must keep pace. Security best-practices call for additional processes, procedures, and technologies beyond those required by the CIP standards."*
- Zpryme surveyed 213 Smart Grid and utility professionals in November of 2012. Over half (52%) of the respondents believed that IT-based solutions alone were insufficient for securing the electrical grid.

WANG & ASSOCIATES
Security & Compliance Consulting

Get Ahead of the Compliance Curve

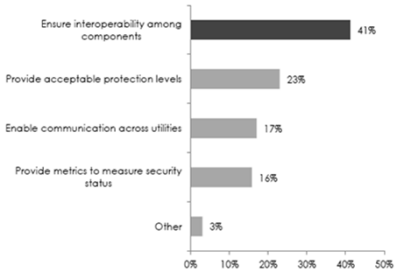
When considering electrical networks in the U.S. as a whole, only 4% of the sample believed they were very secure. Forty-three percent said the networks were somewhat secure, 39% said somewhat insecure, and 15% said very insecure.

Overall, how secure are electrical networks in the U.S.?
(figure 6, source: Zpryme)



The most important role that standards play in implementing security automation technologies was to ensure interoperability among components for 41% of these respondents. Another 23% reported that providing acceptable protection levels was most important, with 17% saying to enable communications across utilities, and 16% saying to provide metrics to measure security status.

What is the most important role that standards play in implementing security automation technologies?
(figure 11, source: Zpryme)



WANG & ASSOCIATES
Security & Compliance Consulting

Electricity Sector Cybersecurity Risk Management Process (RMP) Guideline

- The four (4) stages of the risk management life cycle described in the RMP are:
- **Framing:** provides a framework by which technical risk to critical IT and ICS assets can be put into context with business and organizational needs, ensuring future risk identification and prioritization are considered holistically
- **Assessment:** is the primary process by which risk to business are identified and prioritized.
- **Response:** defines how to address risk based on impact and risk tolerance rather than technical urgency
- **Monitoring:** completes the business improvement loop by ensuring the risk response addressed cybersecurity risk as planned.

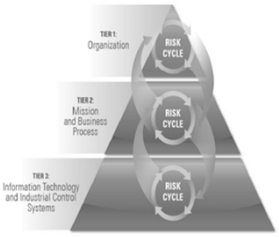


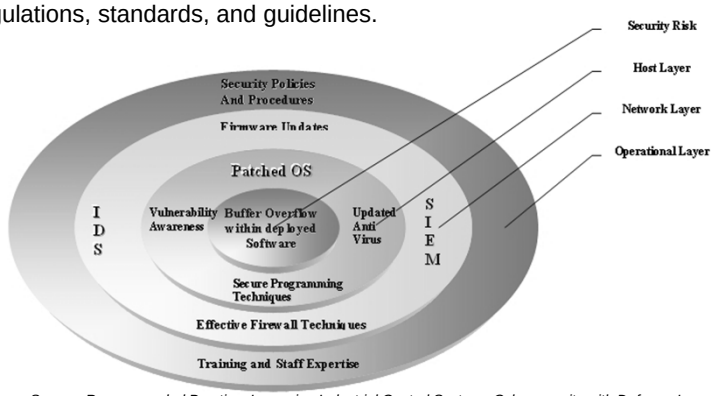
Table 1: Risk Management Process

http://energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf

WANG & ASSOCIATES
Security & Compliance Consulting

Defense-in-Depth Strategy

A Defense-in-Depth Strategy supports confidentiality, integrity and availability of critical controls and related networks, which in turn can be applied to support regulatory compliance towards cyber security regulations, standards, and guidelines.



Source: *Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies*, DHS, October 2009.

WANG & ASSOCIATES
Security & Compliance Consulting

Cyber Security Best Practices

Centralized Account Management Options	Ports & Services	Password Protection	Network Intrusion Detection & Firewall	Security Information Event Management (SIEM)
• Active Directory • MS RADIUS Server • Certificate Authority Server	• Normal Operation • Emergency Operation	• Password Strength • Password Lifetimes • Reuse Restrictions	• Host-based Intrusion Detection System (HIDS) • Detection of Known or Suspicious Network Activity • Application Whitelisting • Redundant Firewalls	• Centralized Real-time Display • Correlates Endpoint Events • Access Control Review • Incident Alert & Alarm • Configuration Management Review • Compliance Audit Trail

WANG & ASSOCIATES
Security & Compliance Consulting

Cyber Security Best Practices

- Define roles and responsibilities in dealing with the ever-changing landscape of securing the utility cyber space. The DHS IT Security Essential Body of Knowledge (EBK) provides a competency and Functional Framework for IT Security Workforce Development.

IT Security EBK: A Competency and Functional Framework

Functional Perspectives
M - Manage
D - Design
I - Implement
E - Evaluate

IT Security Competency Areas	IT Security Roles: Executive: Chief Information Officer	Executive: Information Security Officer	Executive: IT Security Compliance Officer	Functional: Digital Forensics Professional	Functional: IT Systems Operations and Maintenance Professional	Functional: IT Security Professional	Functional: IT Security Engineer	Corollary: Physical Security Professional	Corollary: Privacy Professional	Corollary: Procurement Professional
1 Data Security	M	M D E	E		I	M D E	D E		D E	
2 Digital Forensics		M D	E	M D I E	I					
3 Enterprise Continuity	M	M	E		I	D	E	I	D	
4 Incident Management	M	M D E	E	I	I	D E	D E	I	M D I E	
5 IT Security Training and Awareness	M	M	E				D E		D E	
6 IT Systems Operations and Maintenance			E	D I	M D E	D E		D		
7 Network and Telecommunications Security			E	I	D I	M D E	D			
8 Personnel Security	M	M	E			D E		E	D I	
9 Physical and Environmental Security	M	M	E			D E		M I	D E	
10 Procurement	M	D M E	D E	E	E				E	M D I E
11 Regulatory and Standards Compliance	M	M D E	D E I			I			M D I E	
12 Security Risk Management	M	M D E	D E I	I	I	D I E	I	I	M D I E	
13 Strategic Security Management	M	D M E	D E				D			
14 System and Application Security	M	M	E		I		D E			

WANG & ASSOCIATES
Security & Compliance Consulting

Cyber Security Best Practices

- **In addition to periodic compliance network log review, 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.

- **Address issues regarding ransomware and hacktivists.** Hacker/Broker Agents: Over 137 incidents reported worldwide in 2012 including energy sector organizations. The goals of most hacktivist groups are propaganda and causing damage to achieve notoriety for their cause.

WANG & ASSOCIATES Security & Compliance Consulting

Cyber Security Best Practices

- **Monitor ICS-CERT alerts. Sometimes professional hackers releases exploit code before ICS vendors had the opportunity patch the flaw or offer mitigations.** On January 16, 2013, ICS ICS-CERT has issued an alert about the existence and general availability of the proof-of-concept code for a tool that can brute force passwords and thus gain access and control of programmable logic controllers (PLCs).
- **Disable autorun in SCADA/EMS/HMI systems to prevent malicious codes to execute from USB or other portable devices.** Provide security training on portable devices. US-CERT provides security tips on USB drives at https://www.us-cert.gov/cas/tips/ST08-001.html.

- **Participates in DHS Cyber Storm: Securing Cyber Space biennial exercise** to strengthen cyber preparedness incident response - to examine and refine the roles, responsibilities, authorities, and other key elements for incident recovery.

WANG & ASSOCIATES Security & Compliance Consulting

Cyber Security Best Practices

- **Request industrial control system (ICS) vendors to provide security solution documentation and certifications, factory acceptance test (FAT) measures and site acceptance test (SAT) measures.** DHS' Cyber Security Procurement Language for Control System, September 2009: "The Vendor shall provide an independent third-party security code validation of all Web-based interface software (see Section 5.1). "
- **Request ICS vendors to provide a digital security certificate when issuing future security patch documents or updates so that security personnel can go to the signature panel for Adobe to check for valid and time-stamped signature.**

See an example at:
http://www.gpo.gov/fdsys/pkg/CFR-2011-title18-vol1/pdf/CFR-2011-title18-vol1-sec388-113.pdf

WANG & ASSOCIATES Security & Compliance Consulting

Question & Discussion

Only entities that have the discipline, commitment, and resources; and conduct ongoing training and assessments can foster a secured compliance culture and sustain an audit-ready compliance program.

Send questions and comments to
amwang@wangassoc.com

Thank you!