American Water Works Association

Cybersecurity & the Water Sector

NAWC Water Summit

October 6, 2013

San Diego, CA

Kevin Morley, AWWA

How to deal with Cyber Threat?

- **How would our operations change if we did not have SCADA working?**

- **How sure are we that our SCADA systems are secure?**

- **When was the last time we performed cyber security vulnerability assessments?**

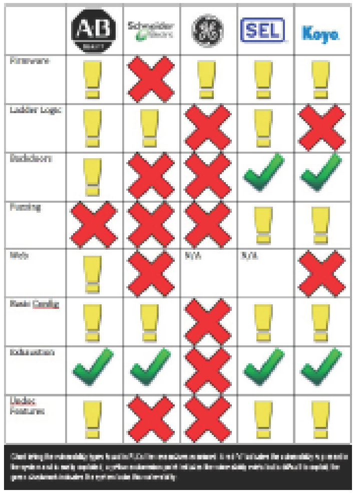
- **What would be the impact to our organizations if we were aware of vulnerabilities and did nothing?**

WIRED

Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software

By Kim Zetter Email Author January 19, 2012 | 7:23 pm | Categories: Hacks and Cracks

The vulnerabilities were found in widely used programmable logic controllers (PLCs) made by General Electric, Rockwell Automation, Schneider Modicon, Koyo Electronics and Schweitzer Engineering Laboratories.



	AB	Schneider Electric	GE	SEL	Koyo
Firmware	!	✗	!	!	!
Ladder Logic	!	!	✗	!	✗
Backdoors	!	✗	✗	✓	✓
Fuzzing	✗	✗	✗	!	!
Web	!	✗	N/A	N/A	✗
Basic Config	!	!	✗	!	!
Exhaustion	✓	✓	✗	✓	✓
Undoc. Features	!	✗	✗	!	!

[illegible]

eWEEK.COM

IT Security & Network Security News

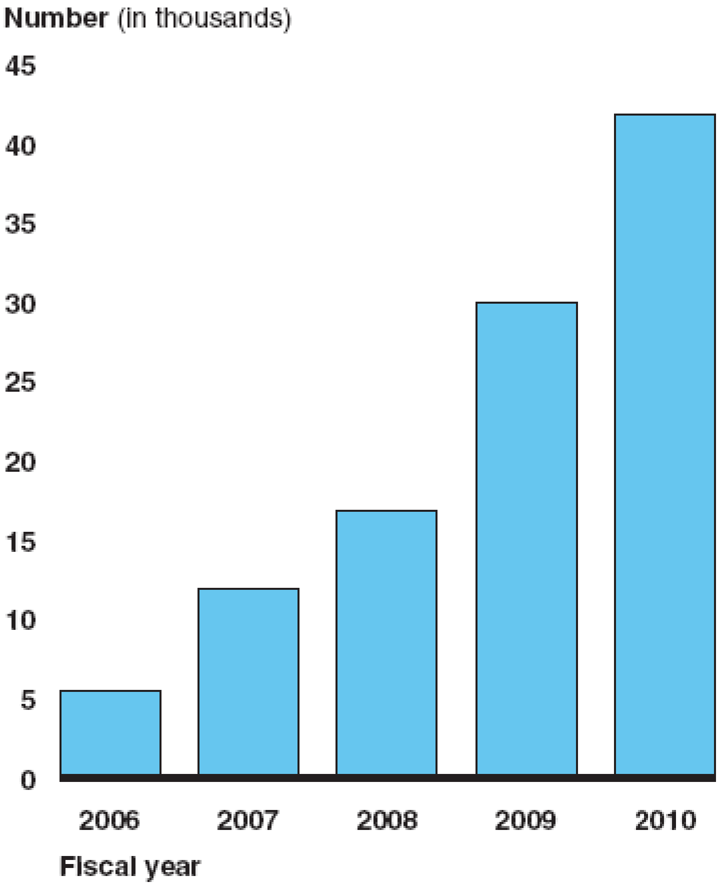
State of SCADA Security Worries Researchers

By: Fahmida Y. Rashid
2012-02-05

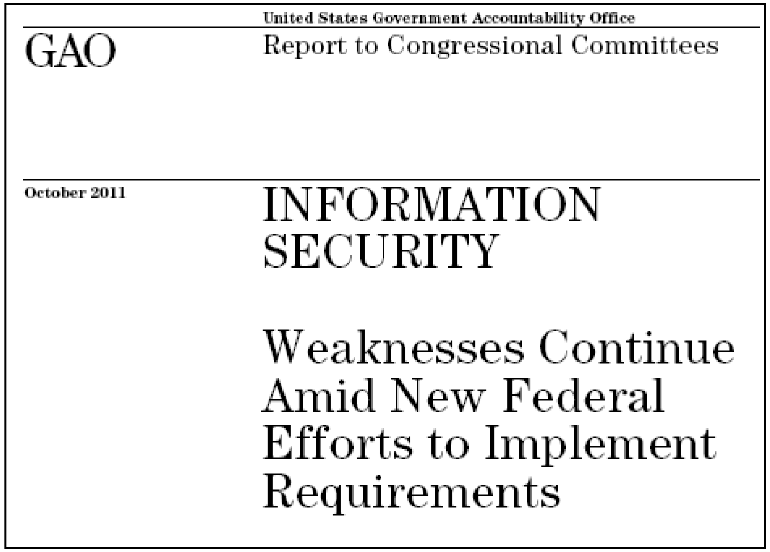
……the work of a different researcher who was able to locate and map more than 10,000 industrial control systems hooked up to the public Internet, including water and sewage plants. While some may have been test systems, some of them were actually in production. Only 17 percent of the systems found asked remote users for authorization to connect, according to that research.

Federal Attention

Figure 1: Incidents Reported to US-CERT, Fiscal Years 2006-2010



Source: GAO analysis of US-CERT data.



United States Government Accountability Office

GAO

Report to Congressional Committees

October 2011

INFORMATION SECURITY

Weaknesses Continue Amid New Federal Efforts to Implement Requirements

So What is the Problem?

Finding

There is no lack of cybersecurity guidance …..[but] given the plethora of guidance available, ***individual entities within the sectors may be challenged in identifying the guidance that is most applicable and effective in improving their security posture.***

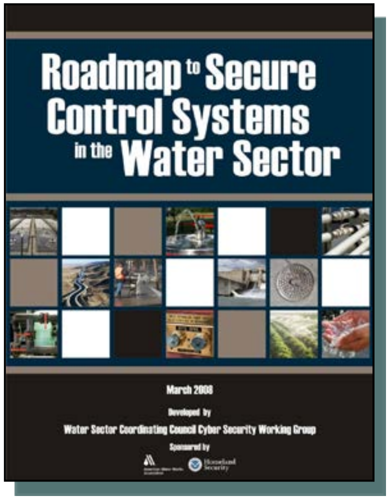
Recommendation

Develop a better understanding of the available guidance and best practices would help both federal and private-sector decision-makers coordinate protection of critical cyber-reliant assets.

Source: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use, GAO-12-92 (http://www.gao.gov/assets/590/587529.pdf)

Water Sector & Cyber Risk

- Y2K
- BT Act 2002



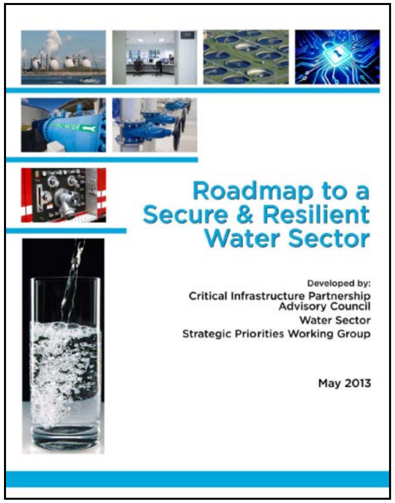
Roadmap to Secure Control Systems in the Water Sector

March 2008

Developed by

Water Sector Coordinating Council Cyber Security Working Group

Sponsored by



Roadmap to a Secure & Resilient Water Sector

Developed by:
Critical Infrastructure Partnership Advisory Council
Water Sector
Strategic Priorities Working Group

May 2013

<u>Critical Milestone</u>
Develop a recommended practices ICS security template for widespread use in the water sector

<u>#1 Priority</u>
Advance the development of sector-specific cybersecurity resources

Moving Forward

Executive Order 13636: Improving Critical Infrastructure Cybersecurity

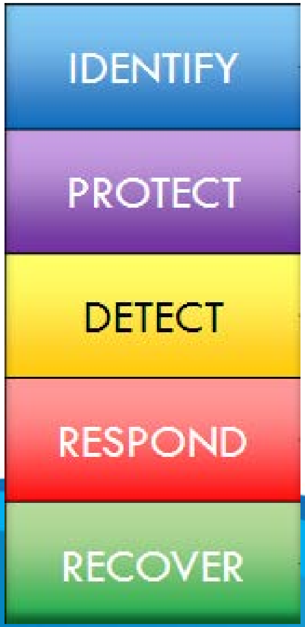
– NIST will lead development of a ***Cybersecurity Framework***

- a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.

– Current draft is function based appoach

– Draft was issued in August 28, 2013

– Final expected in February, 2014



IDENTIFY

PROTECT

DETECT

RESPOND

RECOVER

Water Sector Approach

AWWA WITAF Project #503

- Develop water sector guidance that provides a consistent and repeatable recommended course of action to reduce vulnerabilities in process control systems.
- Target audience for this resource are water utility general managers, chief information officers and utility directors with oversight and responsibility for process control systems.
- Aligns with sector and national priorities, fulfills need for sector-specific guidance as specified in EO 13636.
- Deliverable: *October 2013*

Project Overview

- Project Kickoff – May 1, 2013
- Project Steering Committee
  - AWWA PM – Kevin Morley
  - 3 Water Utility Reps, Consult. Firm, Equip Vendor
- SME Panel
  - 16 Water Utility Reps
  - Vendors & Consulting Firms
  - EPA, DHS, WaterISAC

Project Overview

Current Security Practices survey

- 46 questions
- Online survey administered through AWWA website
- 114 respondents
- Confirmed need for Guidance document
  - Continuing deficiencies in implementation of cybersecurity programs in water sector
  - Limited focus by utility management

Project Overview

Definition Workshop

- Held in Denver on June 25, 2013
- Workshop Objectives
  - Review challenge in raising the importance of protecting control systems against cyber-attack
  - Explore the critical reasons for utilities to focus on this issue and the risks inherent in not doing so.
  - Discuss impediments to utility leadership embracing cyber security as high priority and barriers that get in the way of investing in protection of control systems
  - Develop general framework for the type of cyber security guidance required
  - Define clear communications strategy for ensuring leadership buy-in and successful deployment of AWWA Guidance Document

Project Overview

Recommended Cybersecurity Practices

- 52 practices organized in 12 categories
  1. Governance and Risk Management
  2. Business Continuity and Disaster Recovery
  3. Server and Workstation Hardening
  4. Access Control
  5. Application Security
  6. Encryption
  7. Telecommunications, Network Security, and Architecture
  8. Physical Security of PCS Equipment
  9. Service Level Agreements
  10. Operations Security
  11. Education
  12. Personnel Security

Project Overview

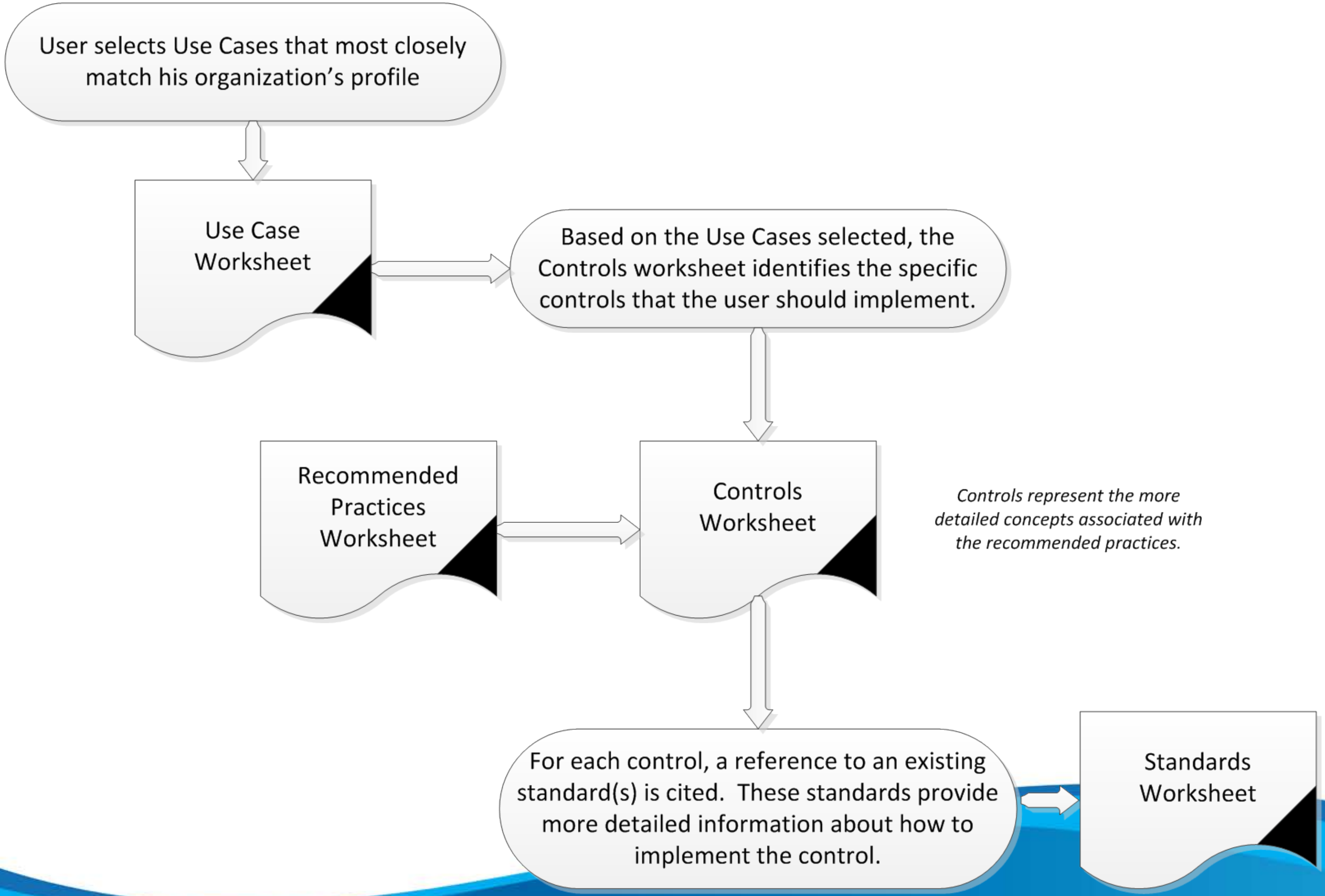
Cybersecurity Guidance for the Water Sector

- PCS Use Cases
  - Characterizes manner in which utility uses PCS and connections to external sources

- Cybersecurity Controls
  - Total of 82 controls
  - More detailed measures needed to implement recommended practices

- References to Existing Standards
  - Paragraph/section number references to set of 9 existing NIST, AWWA, & ISA standards

PCS Cybersecurity Guidance



User selects Use Cases that most closely match his organization's profile

Use Case Worksheet

Based on the Use Cases selected, the Controls worksheet identifies the specific controls that the user should implement.

Recommended Practices Worksheet

Controls Worksheet

Controls represent the more detailed concepts associated with the recommended practices.

For each control, a reference to an existing standard(s) is cited. These standards provide more detailed information about how to implement the control.

Standards Worksheet

Questions

Kevin M. Morley, Ph.D.

Security & Preparedness Program Manager

AWWA – Government Affairs

202-628-8303 or kmorley@awwa.org

www.NationalWARN.org

WARN℠

WATER /WASTEWATER AGENCY RESPONSE NETWORK