Cyber Security
Application to the Water Sector

Rick Hidalgo, PE

Signature Automation

ISA™

Chris Fogle, CISSP

DeltaRisk®
Cyber Security | Business Resiliency | Risk Management

Water/Wastewater Industry Division Webinar
March 6, 2013

Company Backgrounds

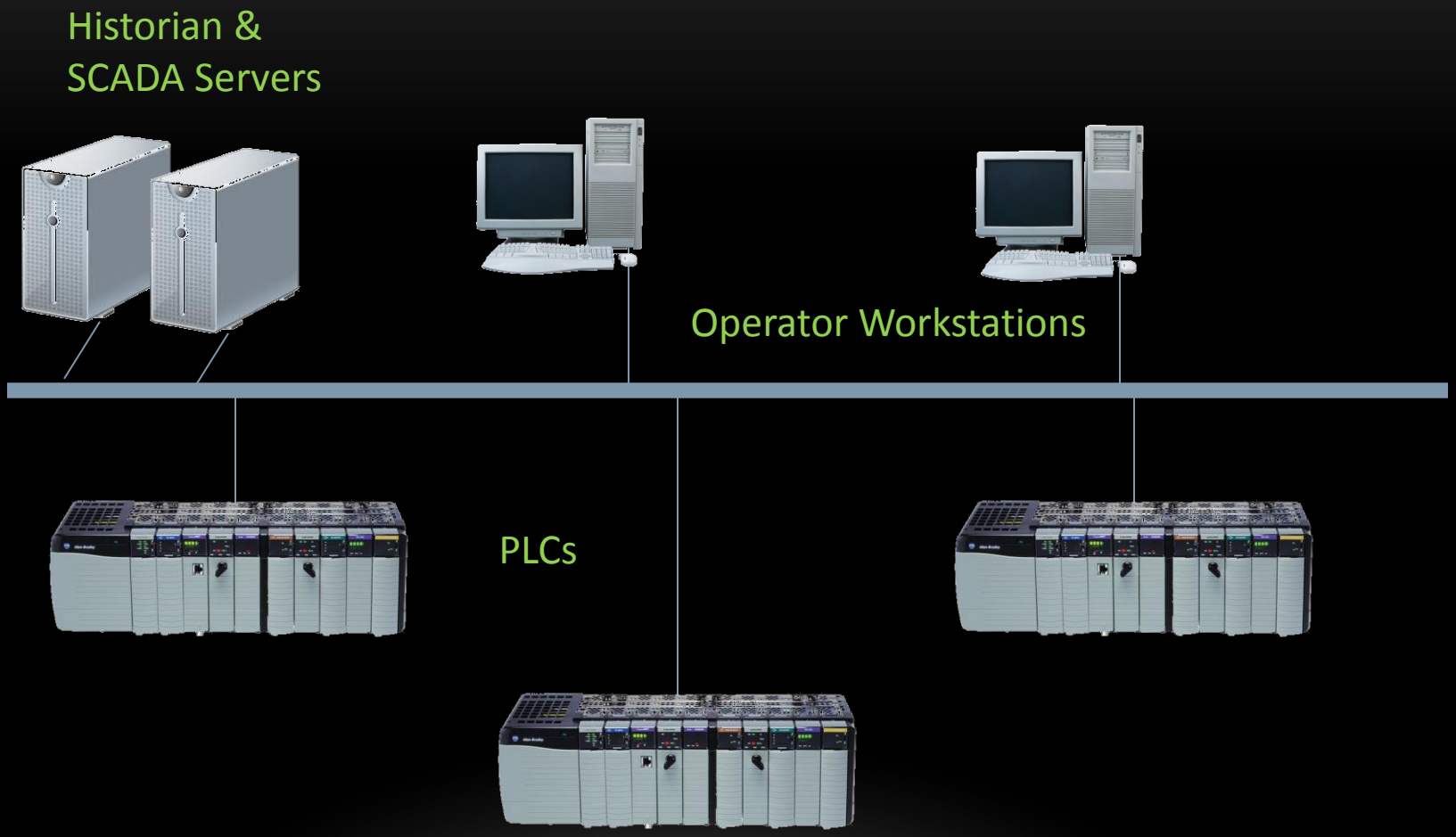
- Founded in 2012 in Dallas, TX
- Licensed Professional Engineering Services Firm
- Founders experienced in providing quality control system solutions for clients across the United States
- Focus on control system planning, programming, configuration and commissioning services
- Wide array of municipal W/WW clients

- Founded in 2007 with offices in San Antonio, TX and Washington, DC
- Focus on countering advanced threats through strategy, policy, analysis, incident response, assessments, training and exercises
- Clients across the globe
  - U.S. National & Homeland Security, Critical Infrastructure Protection, Commercial, International

Today's Agenda

- Control Systems Yesterday and Today
  - Features of Water/Wastewater Control Systems
- Cyber Security and the Water Sector
- Threat Landscape
- FEMA's National Level Exercise 2012
- Emerging Approaches to Securing Critical Infrastructures

Legacy Control Systems



Today's Systems Are More Open And Complex

Features Of Water/Wastewater Control Systems

- Open architecture philosophy
- Numerous communications options
- Considerable use of wireless computing
- No longer isolated from outside connections
- Availability of data to a wide array of users
- High availability and reliability requiring low maintenance
- Easily configurable and non-proprietary
- Ability to leverage IT solutions such as cloud computing, virtualization, etc.

Comparison Of Systems

CONTROL SYSTEMS	IT SYSTEMS
Mixture of protocols	Primarily Ethernet TCP/IP
Limited device security	Enhanced security tools
Wide array of device types	Primarily computers on common OS
Focus on maintaining treatment processes or production	Focus on protecting data
Security must NOT impede operations	Security can override user
24/7 availability	Scheduled outages are acceptable

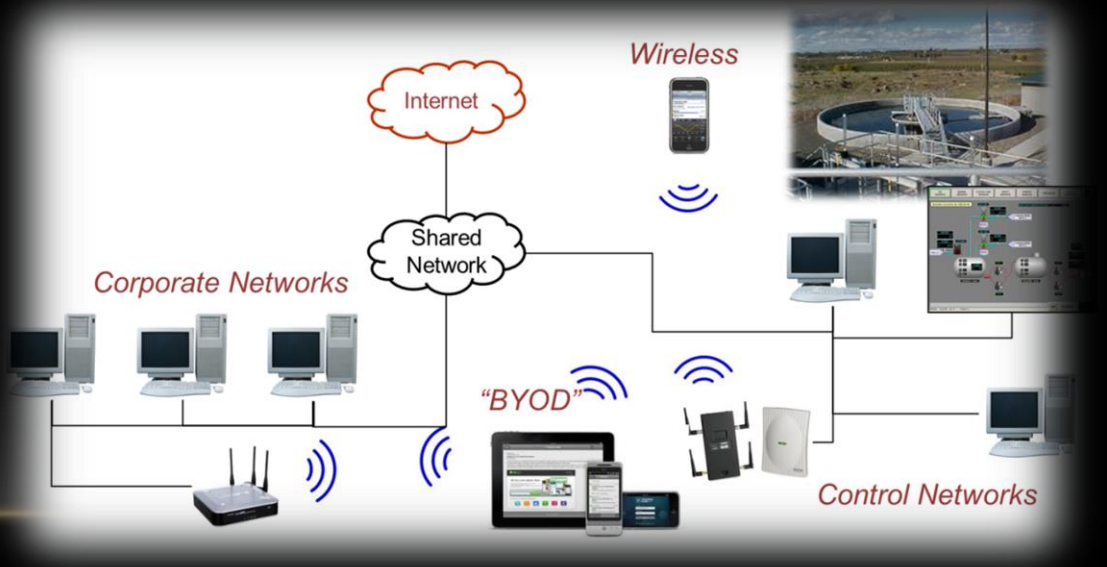
Shifting Security Landscape

"Shared Benefit / Shared Pain"

- Highly-networked
- Open systems architectures
- Shared communications
- Well-known protocols
- Mobile and wireless
- Convenience of BYOD

"Security through Obscurity"

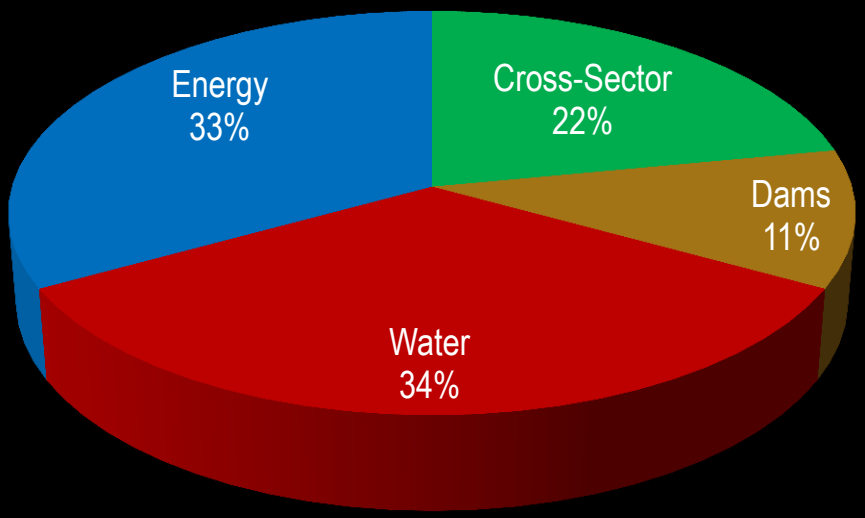
- Stand-alone
- Obscure protocols
- Dedicated comms.



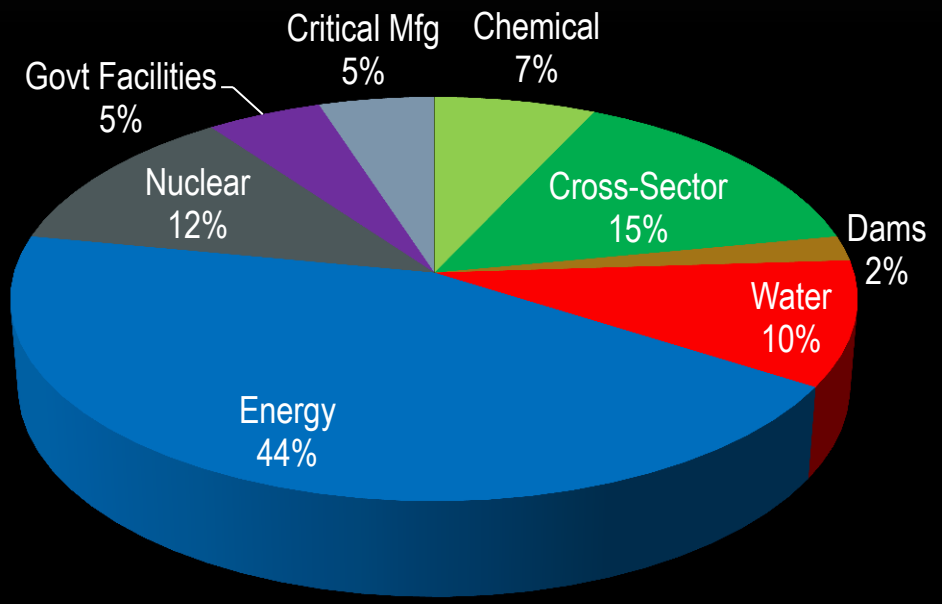
Why Is Cyber Security Important?

Reported Events In The Water Sector

2009 - 3 Water Incidents



2010 - 4 Water Incidents



Source: ICS-CERT Incident Response Summary Report 2009–2011

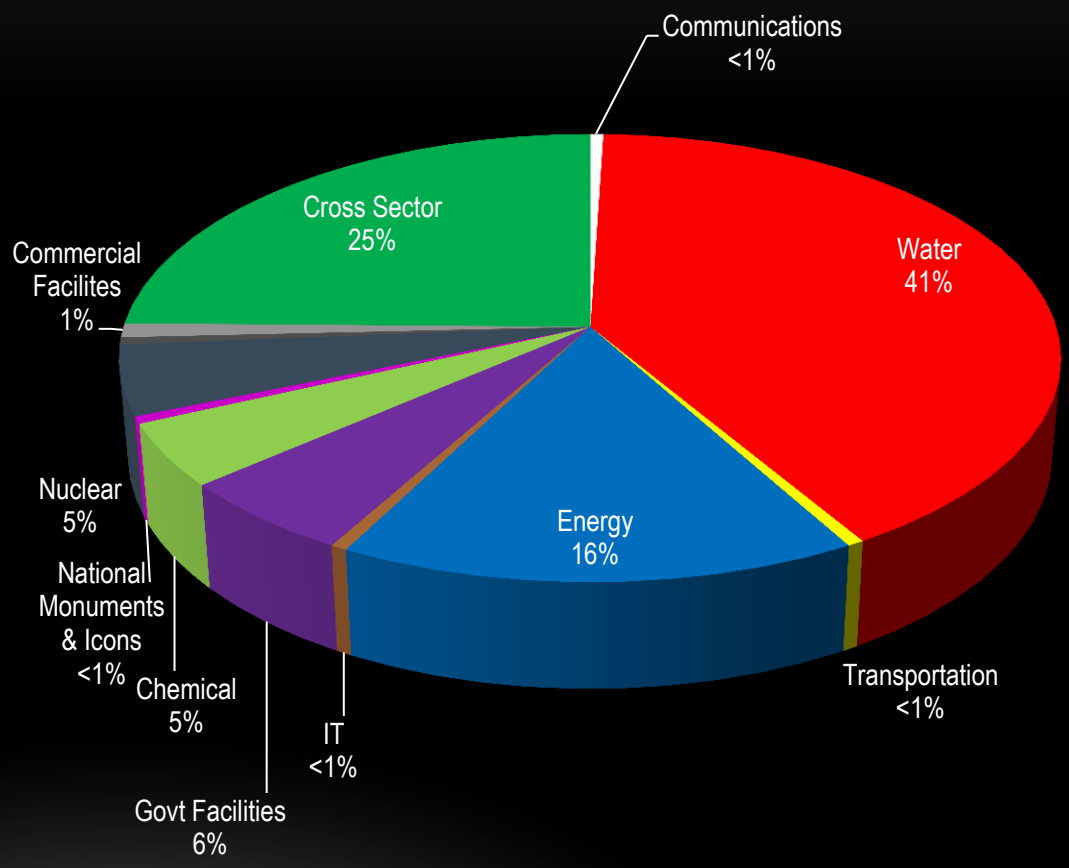
2011 Increase In Water Incidents

… due to a large number of Internet facing control system devices reported by independent researchers

… remote access platform from the same vendor, configured with an unsecure authentication mechanism

… risks associated with weak boundary protection practices

2011 - 81 Water Incidents



Source: ICS-CERT Incident Response Summary Report 2009–2011

Shhhhh…it's A Secret!

"Cyber incidents are most commonly kept secret when discovered, leaving customers, and policymakers in the dark about frequency, impact and root causes."

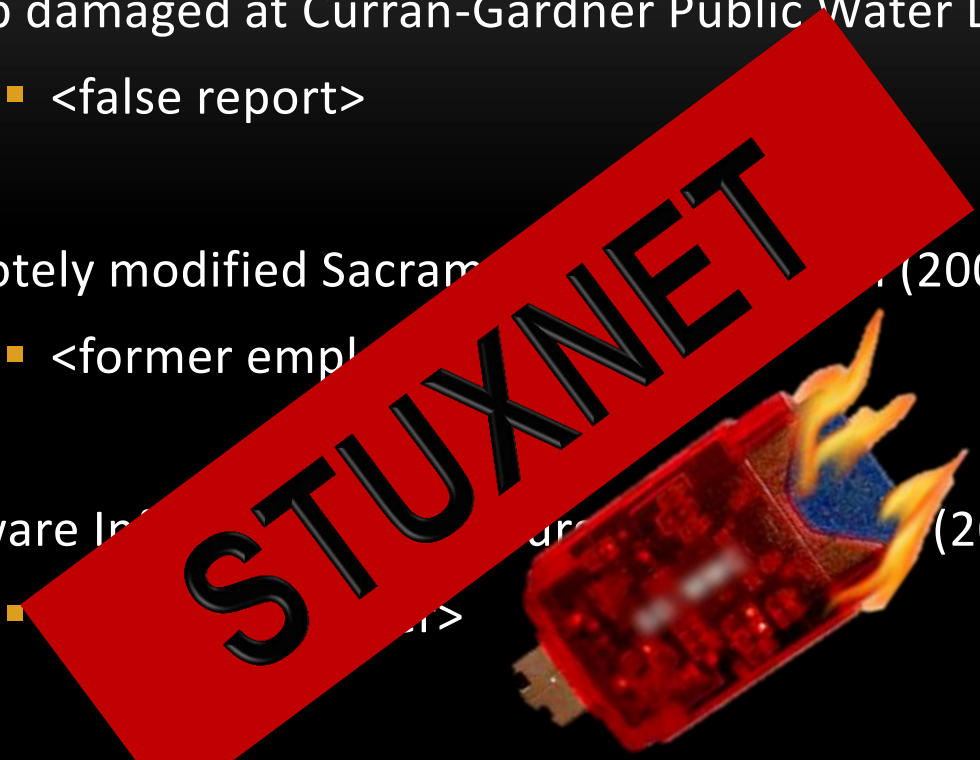
Source: European Network and Information Security Agency (ENISA) – August 27, 2012

Cyber Threats and Incidents In Water/Wastewater

- Pump damaged at Curran-Gardner Public Water District (2011)
  - <false report>
- Remotely modified Sacramento River control (2007)
  - <former employee>
- Malware Infection at Harrisburg Water System (2006)
  - <overseas hacker>
- Sewage Spill at Maroochy Shire (2001)
  - <disgruntled job applicant>

Cyber Threats and Incidents In Water/Wastewater

- Pump damaged at Curran-Gardner Public Water District (2011)
  - <false report>
- Remotely modified Sacram (2007)
  - <former empl
- Malware In dr (2006)
  - r>
- Sewage Spill at Maroochy Shire (2001)
  - <disgruntled job applicant>



Common ICS Vulnerabilities

PRODUCT

- Improper Input Validation
- Indicator of Poor Code Quality
- Permissions, Privileges & Access Controls
- Improper Authentication
- Insufficient Verification of Data Authenticity
- Cryptographic Issues
- Credentials Management
- ICS Software Security Config & Maintenance

CONFIGURATION

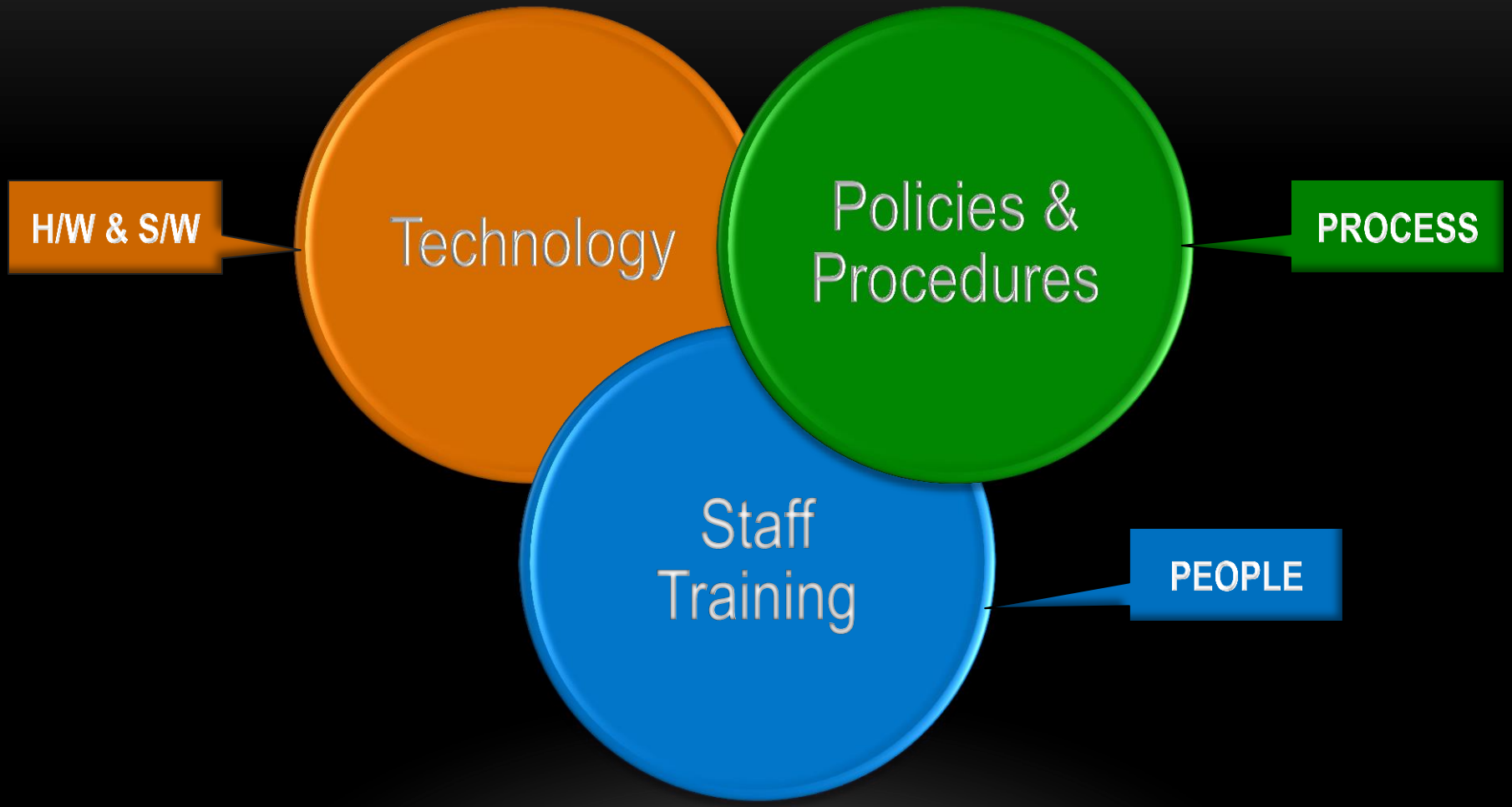
- Permissions, Privileges & Access Controls
- Improper Authentication
- Credentials Management
- ICS Software Security Config & Maintenance
- Planning/Policy/Procedures
- Audit and Accountability (Event Monitoring)

NETWORKING

- Audit and Accountability (Event Monitoring)
- Network Design Weaknesses
- Weak Firewall Rules
- Network Implementation Shortcomings

Source: DHS' Common Cyber security Vulnerabilities in Industrial Control Systems – May 2011

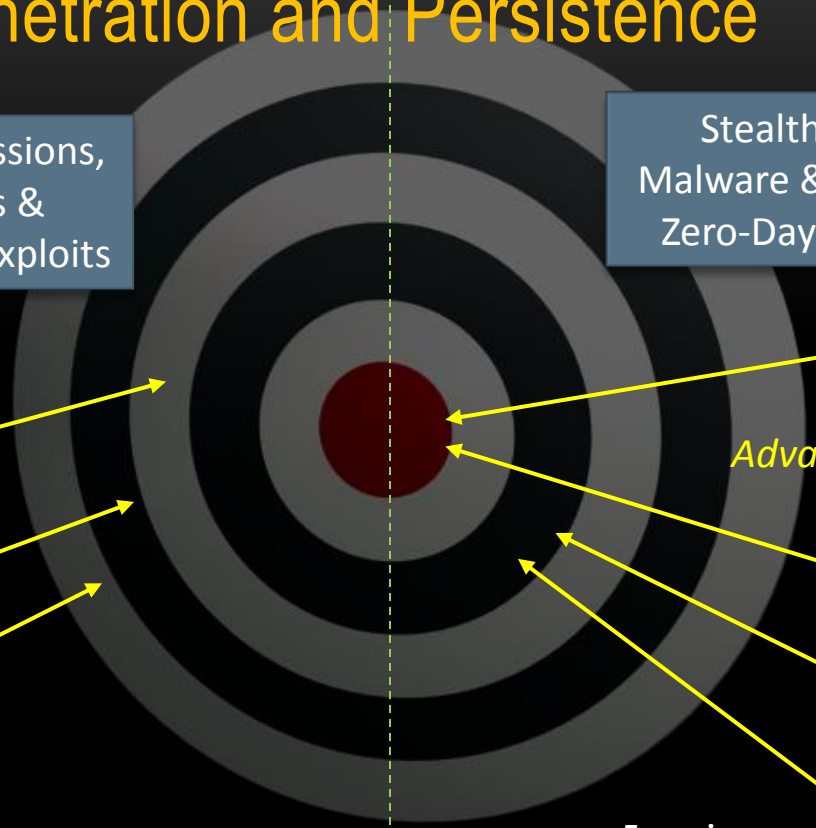
Key Areas For Addressing Cyber Security



Increasing Penetration and Persistence

Denial of Service, Hijacked Sessions, Web Defacements, Viruses & Malware, Known or One-Off Exploits

Stealthy Infiltration, Embedded Malware & Agents, Social Engineering, Zero-Day Exploits, Rapidly Changing



Hacker Groups

Hacker

Script Kiddies

State-Supported

Advanced Persistent Threat (APT)

Corporate / Criminal

Cyber Terrorist

Hacktivists

"1st Generation" Information & Network Security

- Security by prevention
- System & software vulnerability assessment
- Penetration testing
- Respond to most-recent event
  - Effectiveness rarely assessed
  - Prepared for the "last war"
- Hyper focus on technology & compliance

Emerging "2nd Generation" Threats

- Quickly evolving; seeks asymmetric advantage
- Persistent & patient; waging long-term campaigns
- Structured organization & planning
- Well-resourced (money, people, skill)

Rising Concern Across Critical Infrastructure Sectors

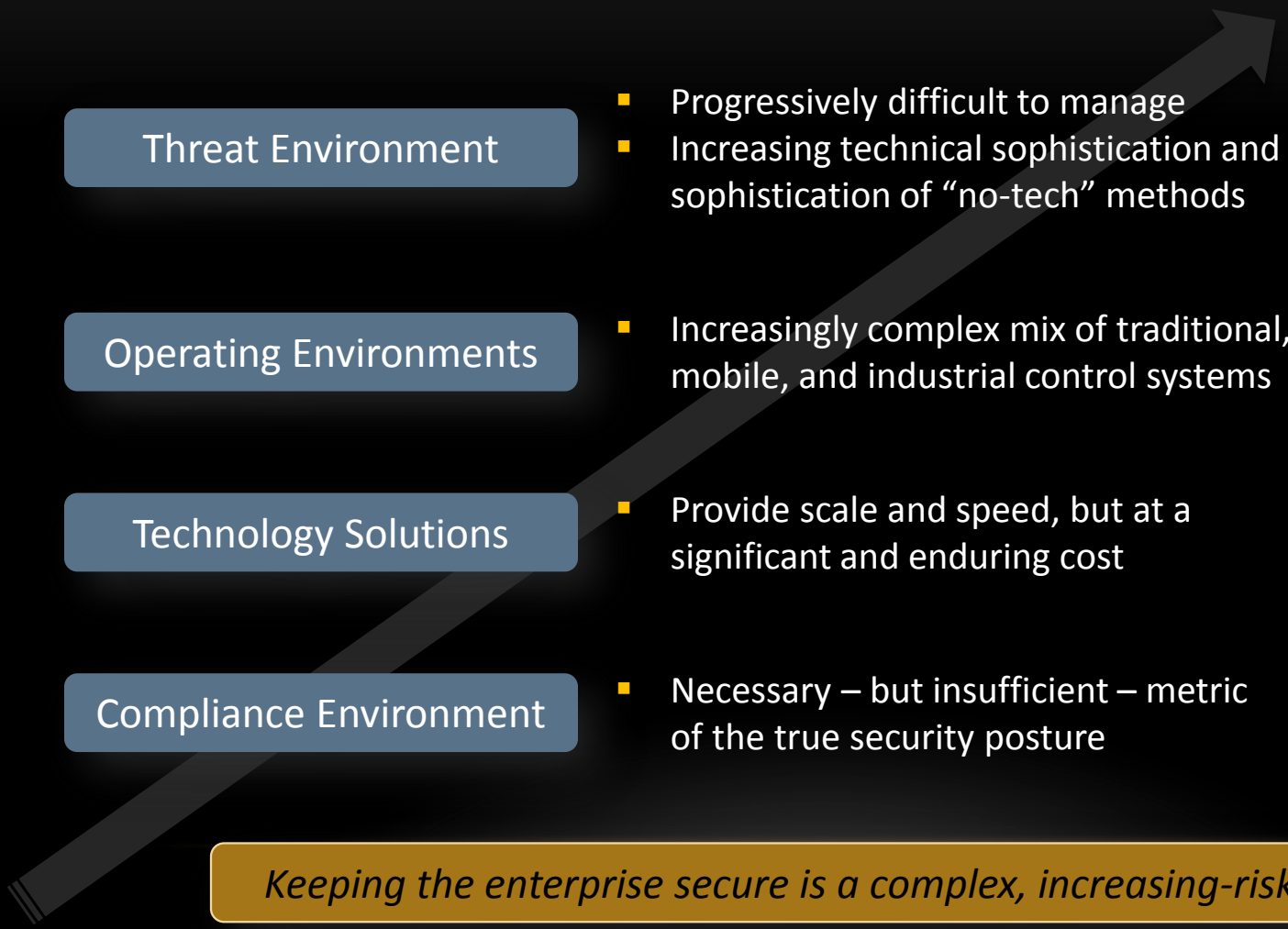
- **As national security issue / as corporate challenge**
  - First tier national security issue
    - DoD assumes it is unstoppable – goal is to manage risk/mitigate
    - Deep concern over private sector readiness
    - Financial services and other critical infrastructure sectors often highlighted as key target
  - Corporate response varies widely; most mature in Defense Industrial Base (DIB); then Financial Services

- **Intersection of cybersecurity and Industrial control systems / automation**
  - Historically on the electric power transmission and distribution, pipelines, and chemical production
  - Emerging Focus on logistics and other transportation modes
    - Example: Postal, Shipping, Logistics
  - Key consideration in ability to support force deployment and sustainment (DoD), national emergency response (DHS, FEMA)

Threats

- Poor general cyber security practices
  - Misconfigured devices
  - Using default passwords
  - Weak passwords
  - Shared logins
  - Unrestricted physical access
  - Poor patch management / unpatched systems
  - Unused open accounts
  - Weak enforcement of remote login policies
  - Weak “thumb drive” practices
- Unmanaged mobile devices and weak BYOD policies
- Weak security awareness training for staffs
- Weak network security
  - Network design weaknesses; lack of functional DMZs and segmentation
  - Lack of intrusion detection, misconfigured firewalls
  - Insufficient security logging and review
  - Insufficient monitoring
- Weak policies and programs
  - Lack of security assessments and enforcement of policies
  - Insufficient “cyber” disaster recovery preparation and testing
  - Lack of critical plans and other documentation
- Unmonitored access and weak security practices of vendors and suppliers
- Public access to sensitive information – contracts, schematics, equipment lists, personal information

Increasing Complexities: "Realities" Of Enterprise Network Security



Threat Environment

- Progressively difficult to manage
- Increasing technical sophistication and sophistication of "no-tech" methods

Operating Environments

- Increasingly complex mix of traditional, mobile, and industrial control systems

Technology Solutions

- Provide scale and speed, but at a significant and enduring cost

Compliance Environment

- Necessary – but insufficient – metric of the true security posture

Keeping the enterprise secure is a complex, increasing-risk proposition

FEMA's National Level Exercise 2012

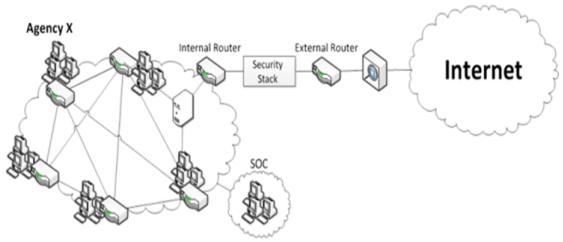
	Exercise #1: Information Exchange	Exercise #2: Cyber Incident Management	Exercise #3: NLE Capstone/ Cyber Physical Effects	Exercise #4: Continuity Exercise
Timeframe	March 2012	April 2012	June 2012	June 2012
Scope	▪ Discussion-based ▪ Cyber Unified Coordination Group ▪ Cyber Operations Centers	▪ Discussion-based ▪ Part I: National Tabletop Exercise (NTTX) to examine National Cyber Incident Response Plan (NCIRP) ▪ Part II: Senior-Level Exercise	▪ Regions I, II, III, V, and the D.C. area ▪ Operations-based ▪ Whole Community ▪ Simultaneous testing of National Response Framework and NCIRP ▪ Broader participation	▪ Operations-based ▪ Emergency Relocation Groups (Federal) ▪ Selected regions and states
Focus Areas	▪ Information exchange	▪ Examining the NCIRP from the strategic to the operational level	▪ Strategic decisions ▪ Activation of operations centers ▪ Operational decisions	▪ Relocation ▪ Devolution ▪ Communications

FEMA's National Level Exercise 2012

High-Level Design Goals

- **Impacts across** the USG, CIKR Sectors, States, International and other organizations;
- **Ambiguous threat landscape**;
- **Physical impacts** resulting from cyber attack and cascading effects;
- **Effects** to critical logistics and data, industrial control systems and associated operations;
- ***"Threat of…"* attacks** to drive wide-ranging analysis, planning, and implementation of protective measures among public and private stakeholders; and
- Conditions that demonstrate the need for **timely decision making** with respect to protective measures and cyber responses.

- Information Technology
- Communications
- Public / Municipal Services
- Government Facilities and Networks



Scenario Elements

- Cyber Intrusions, Botnets, Malware, Phishing Attacks
- Backbone IT infrastructures
- Cloud Services, Enterprise and Mobile Networks
- Industrial Control Systems and Production Networks

Combined adversaries' actions would result in disruptive and/or destructive impacts across a number of CI/KR sectors

- Managing responses to intrusions
- Mitigating effects of malware on mission critical systems and services
- Responding to US-CERT guidance and coordinating enterprise response options
- Managing effects due to the compromise of sensitive information
- Operations in a "cyber degraded" environment
- Information-sharing capabilities internal and external to all sectors
- Coordination of cyber incident management with private-sector CI/KR owners and operators

NLE 2012 And The Water Sector

- Notional attacks against local distribution operations
  - National Capital Region/U.S. Army Corps of Engineers, New Jersey, Massachusetts, Rhode Island, Maine, New Hampshire, Michigan
  - SCADA networks in the Eastern U.S. … use of specially-crafted malware … infections of programmable logic controllers (PLCs) .. masking of feedback … malfunctioning of the system
  - Notional impacts included pump overspeed conditions, outages affecting cooling capabilities in data centers and availability of water for fire suppression systems. … valve failures impacting water quality
- Water-ISAC instrumental in facilitating information sharing and sector participation
  - Cross-sector dependencies; and separating “fact” from “fiction” with regard to threats, vulnerabilities, and likelihood of impacts in the sector

Changes Occurring…?

- NLE reflected continuing concerns about critical infrastructure and control system security
  - Water sector now in “top 5” of CIP attention (power grid, pipelines, gas/oil production, water/waste water, logistics)
- W/WW companies must confront convergence of control systems and open (traditional) IT infrastructures and technologies
  - Inherited vulnerabilities; wider “attack surface”; older systems with generally poor built-in security
  - Increasingly joined administrative and control networks
  - Access to the control side via mobile devices
  - Stiff liabilities and public reaction to compromises
- Addressing the general absence of robust network security
  - Boundary protection, intrusion detection, threat analysis, incident response, internal monitoring, insider threats, security assessments, security training, business continuity

Framing Context

Most large enterprises employ "1st generation defenses" against "next generation threats"

Technology is advancing; training and tactics have not

Focus on balanced fusion of people, processes & technology

Frequent, hands-on, realistic training; tailored assessments

Incorporating advanced training, exercises, and assessments gives an enterprise capabilities it needs to counter sophisticated threats

Key Enablers of Advanced Defense

- Information sharing
- Collaborative threat analysis
- Assessments "inside the castle wall"
- Incident response
- Training and workforce development
- Exercises

Targeted “First Step” Best Practices

1. Facilitated risk discussions / tabletop exercises
   - Leadership, managers, technical staff, key vendors
2. Staff training and awareness
   - Current threats, technical mitigation, general cybersecurity skill-building
3. Security Survey
   - Assessing current practices and comparing to known and emerging trends; interviews, surveys, and team observations in seven (7) key program areas in cyber security:
     - Governance, Cyber Risk Management, Technology Ecosystem, Operational Practices, Threat Awareness, Analysis Capabilities, Capacity Growth and Resilience

Thank You For Your Time

Rick Hidalgo, P.E.
hjhidalgo@sig-auto.com
469-248-6840
www.signature-automation.com

Chris Fogle, CISSP
cfogle@delta-risk.net
210-293-0707
www.delta-risk.net