BlackRidge TECHNOLOGY

End-to-End Trust, Segmentation and Segregation in the "IIoT"

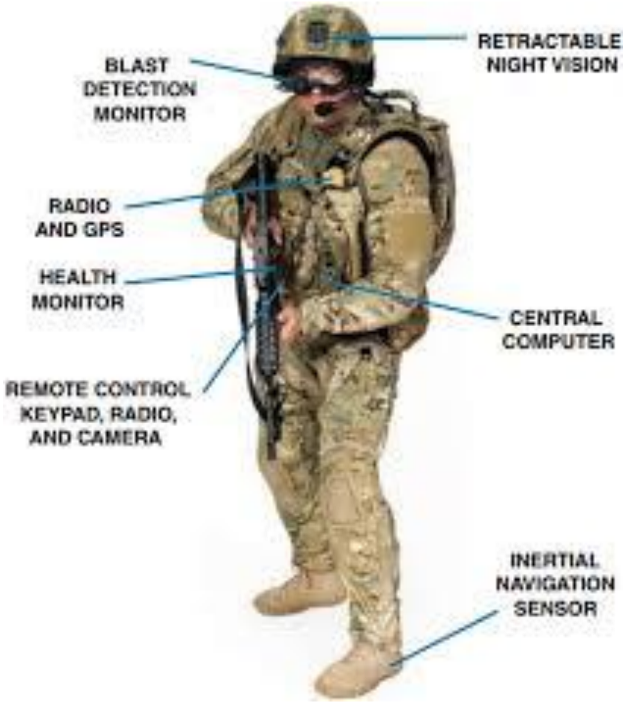
Michael Murray - SVP & GM Cyber Physical Systems

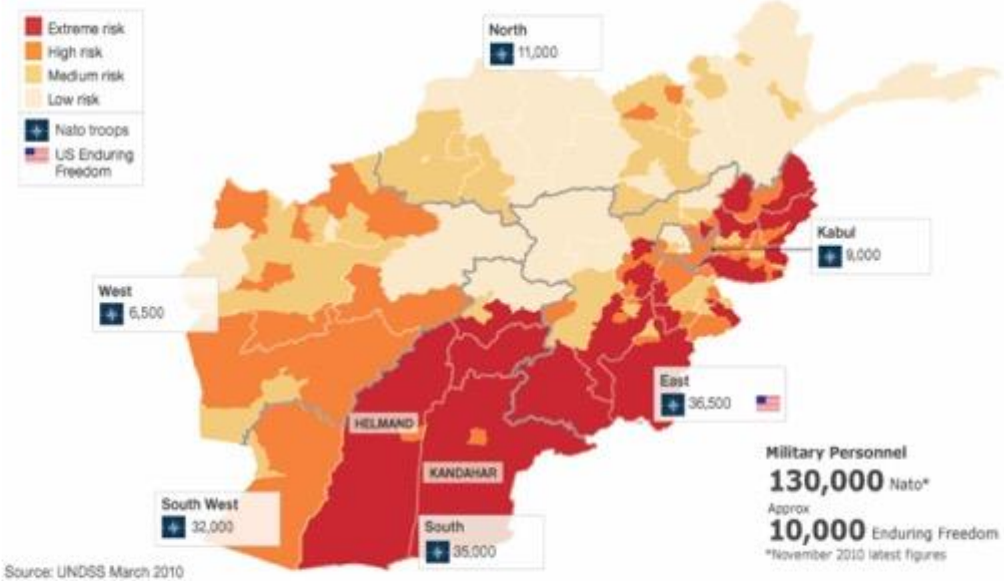
www.blackridge.us

Company Origin

BlackRidge technology originated from a Department of Defense contract to cloak IP Connected devices used in the Afghanistan war

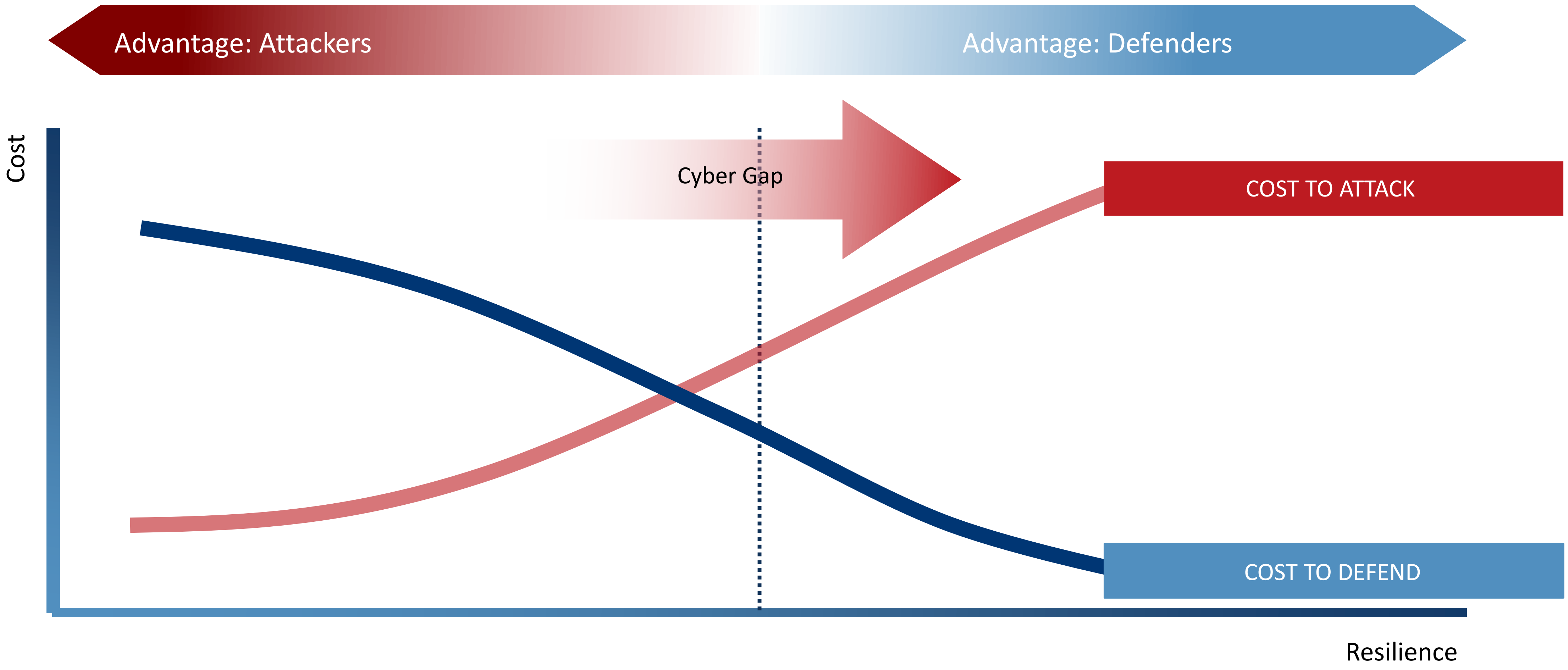
The average US soldier carries greater than six vulnerable points of network connectivity





Source: UNDSS March 2010

End Game: Resilient Architectures Require Economic Asymmetry



BlackRidge TECHNOLOGY

PRESIDENTIAL EXECUTIVE ORDER ON
STRENGTHENING THE CYBERSECURITY OF FEDERAL
NETWORKS AND CRITICAL INFRASTRUCTURE

Security Tip (ST18-001) Securing Network Infrastructure Devices

NCCIC encourages users and network administrators to implement the following recommendations to better secure their network infrastructure:

- ***Segment and segregate networks and functions.***
- ***Limit unnecessary lateral communications.***
- Harden network devices.
- ***Secure access to infrastructure devices.***
- ***Perform Out-of-Band network management.***
- Validate integrity of hardware and software.

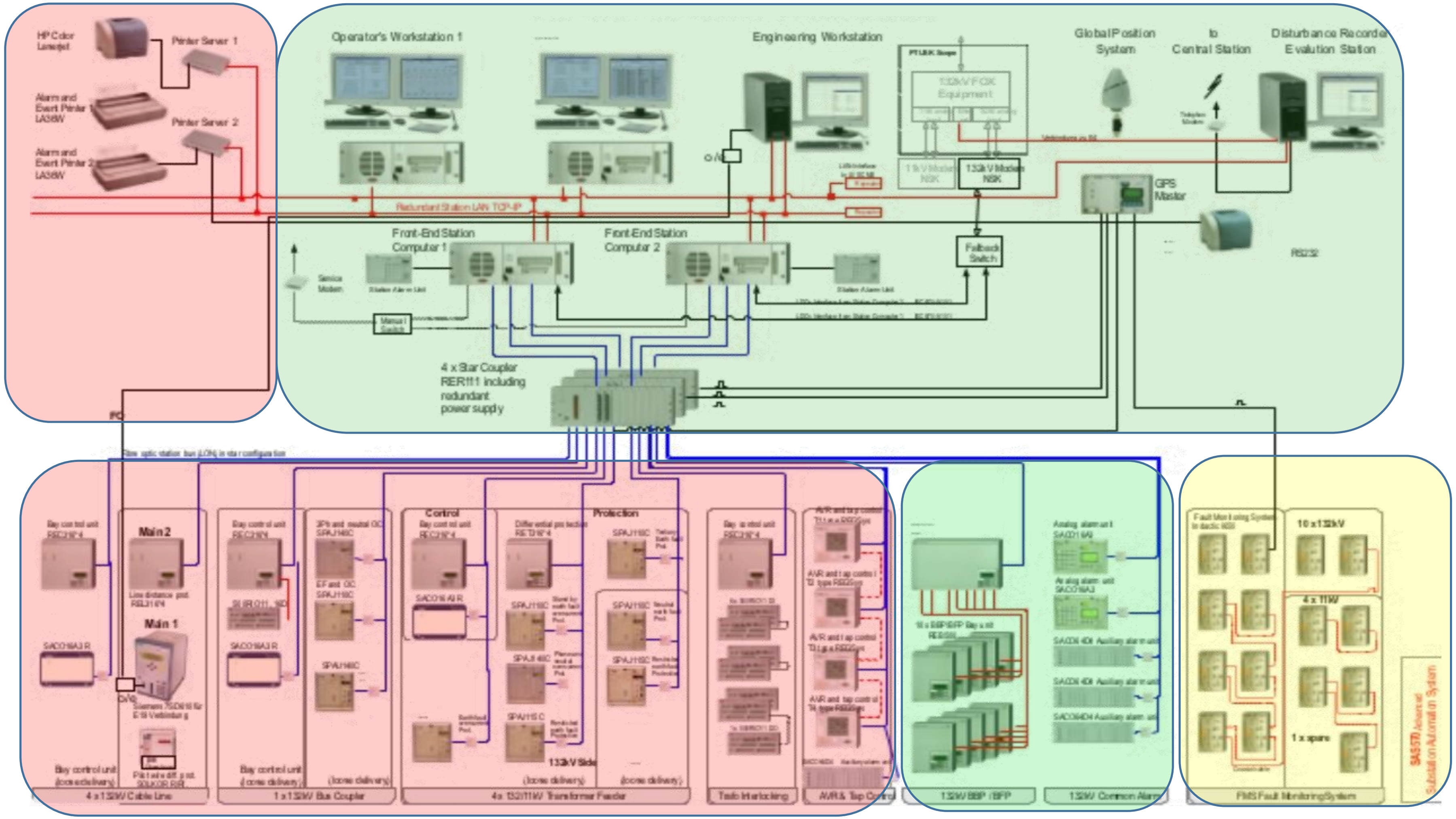
Segment and Segregate Networks and Functions

Security architects must consider the overall infrastructure layout, including segmentation and segregation. Proper network segmentation is an effective security mechanism to prevent an intruder from propagating exploits or laterally moving around an internal network. On a poorly segmented network, intruders are able to extend their impact to control critical devices or gain access to sensitive data and intellectual property. Segregation separates network segments based on role and functionality. A securely segregated network can contain malicious occurrences, reducing the impact from intruders in the event that they have gained a foothold somewhere inside the network.

Technical Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Segmentation/Segregation of all Layers

New Systems can exist with legacy systems through Segmentation and Segregation.



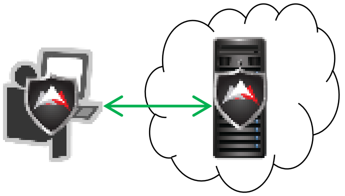
What Can the Community of Interest do to Respond?

Protect Critical Servers and Management Systems

- Protect high value servers and data (PII, algos, research, IP, ….)
- Protect Management Plane of IT networks and systems
- Data centers, IaaS cloud services, and IoT

Isolate and Protect Cloud Services

- Control access to IaaS cloud servers by all parties
- All access attempts logged for audit history with attribution
- No unauthorized awareness of public cloud services



Micro-Segmentation / Software-Based Segmentation / Compliance

- Infrastructure independent and supports heterogenous environments
- Separates security policy from network topology
- Addresses compliance, risk and regulatory requirements

Identity-Based Networking

- Identity Based Policy and Network Access
- Topology Independent Networking

Cybersecurity: Compliant or Complacent?

Nicholas W. Santillo Jr.

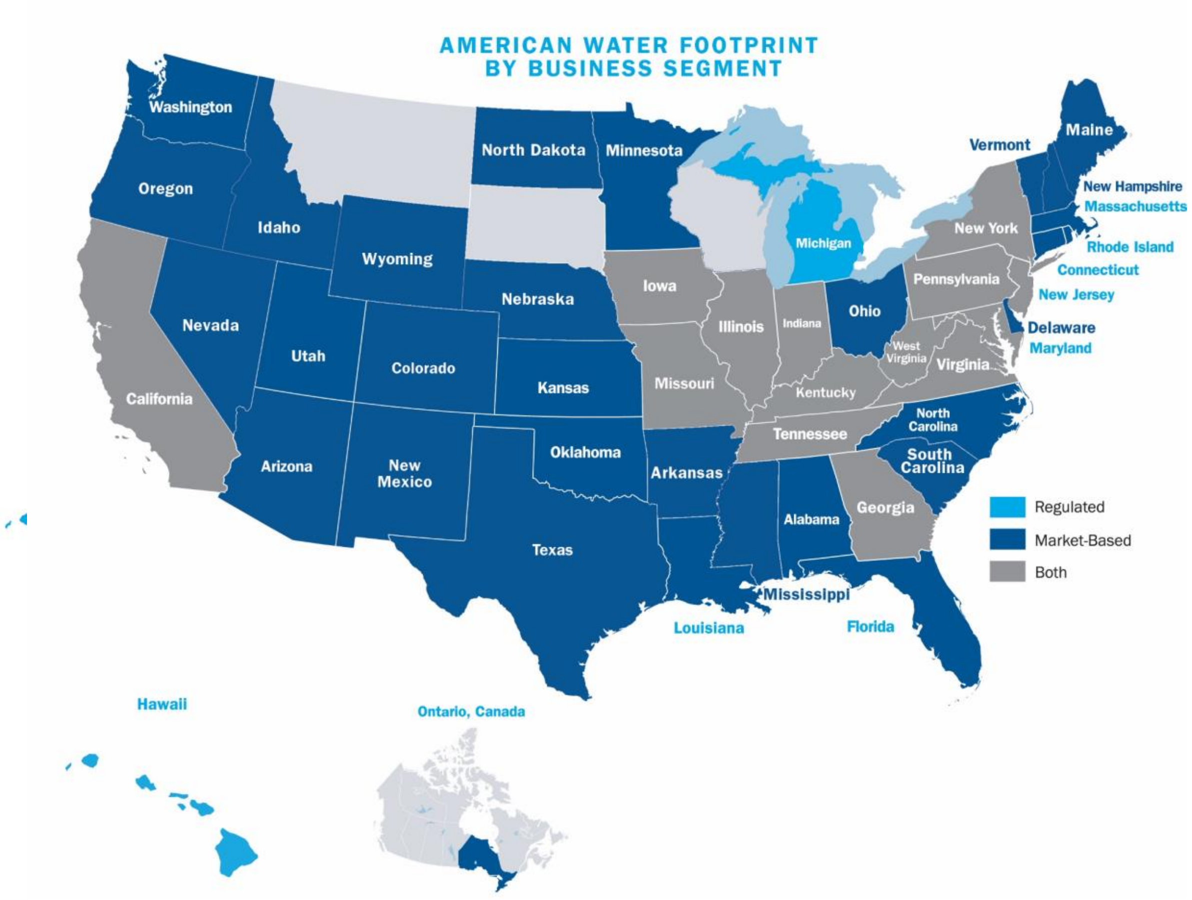
Chief Digital Infrastructure & Security Officer

American Water

WHO WE ARE

We are the largest and most geographically diverse publicly traded water and wastewater service provider in the Unites States.

- We serve a broad national footprint and a strong local presence.
- We provide services to approximately 14 million people in **45 states** and Ontario, Canada.
- We employ **7,100** dedicated and active employees and support ongoing community support and corporate responsibility.
- We treat and deliver more than **one billion** gallons of water daily.



Water Sector Road Map – Top Priority Cyber Risk Management

Water Sector Challenges:

- Complex and Evolving Cyber Vulnerabilities

- Increased Automation of Operational and Business Functions

- Difficult to keep up with increasingly sophisticated Cyber Threats

Our Digital Risk Program

Program Components

NIST Cyber Security Framework

Threats & Digital Risk Management

Critical Systems & Technical Controls

Partnerships and Information Sharing

Incident Response Capability

Education Training & Awareness

Industry Leadership & Cyber Innovation

Digital Risks

System Vulnerabilities

Breach of Sensitive Information

Advanced Persistent Threat

Malicious Insider

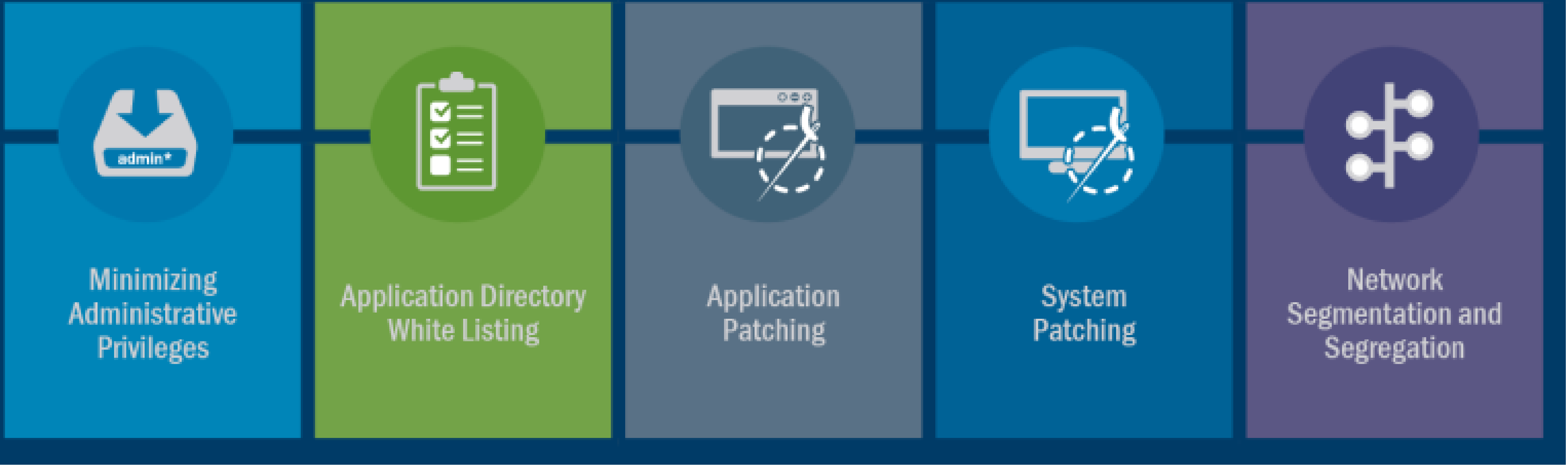
Third Party Risks

Basic Cyber Hygiene – US-CERT Top 5

Basic Cyber Hygiene would prevent approximately 85% of security breaches

0 ZERO DAY exploits in major breaches over the last 24 months.

“National Security Agency”


admin*
Minimizing Administrative Privileges
Application Directory White Listing
Application Patching
System Patching
Network Segmentation and Segregation

Resources / Partnerships

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

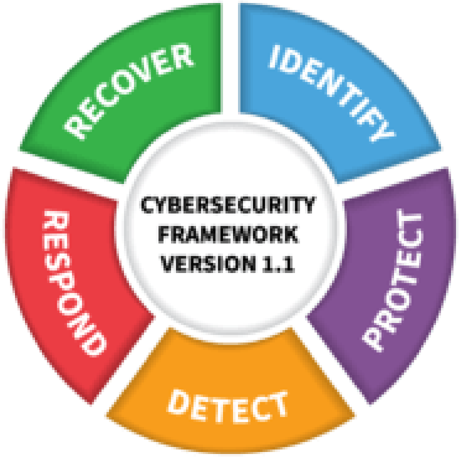
C3 VOLUNTARY PROGRAM

CSET®
CYBER SECURITY EVALUATION TOOL

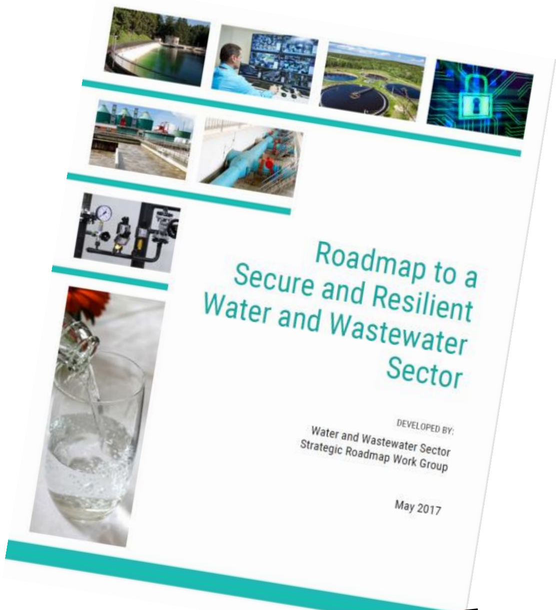
- Cyber Security Advisors (CSA)
- Protective Security Advisor (PSA)
- National Cybersecurity Assessment & Technical Services (NCATS)
- Cyber Information Sharing and Collaboration Program (CISCP)
- Design Architectural Review (DAR)
- Network Architecture Verification and Validation (NAVV)

EPA United States Environmental Protection Agency

CYBERSECURITY FRAMEWORK

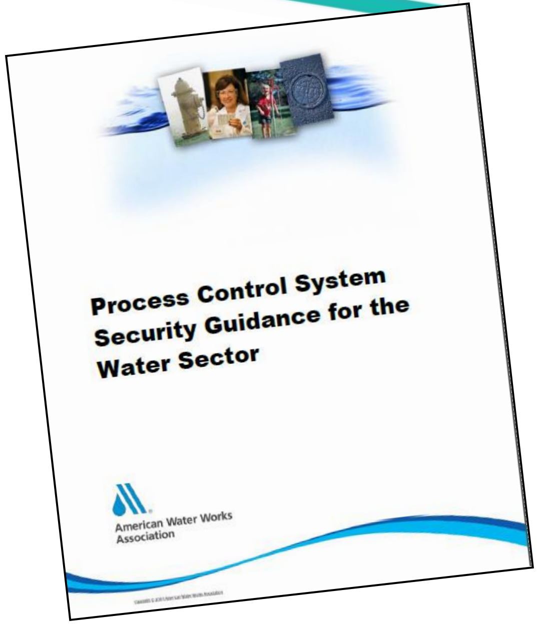


WATER ISAC


Roadmap to a Secure and Resilient Water and Wastewater Sector

DEVELOPED BY:
Water and Wastewater Sector Strategic Roadmap Work Group

May 2017


Process Control System Security Guidance for the Water Sector

American Water Works Association

THANK YOU