Conducting Cyber Risk Assessments under AWIA:

A WaterISAC Webinar Series

Webinar #1
Introduction to the Cybersecurity Assessment Process

July 17, 2019

WaterISAC Mission

Protect Utilities

Information sharing

Background

- Established in 2002 at the urging of the White House, FBI and US EPA
- Created by the water and wastewater sector
- Focused solely on the sector's security needs
- Dues-based non-profit

Areas of Focus

- Physical Security
  - –Terrorism
  - –Other malicious activity
- Cybersecurity
  - –Business/Enterprise System
  - –Industrial Control System
- Natural Disasters
- Other Hazards

Information Gathering, Curation, Analysis & Dissemination

Membership

- Water and wastewater utilities
- Consulting and engineering firms
- Local, state and federal agencies

- Dues: tiered based on size and organization type
- 60-day free trial membership
- Join at waterisac.org

Presenters

- **Terry Draper**, PE, PMP
  EMA, Inc.

- **Jeff Coulson**, MMSc, P. Eng, PMP
  EMA, Inc.

- www.ema-inc.com

Introduction to the Cybersecurity Assessment Process

July 17, 2019

Jeff Coulson
Director, EMA

Terry Draper
Vice President, EMA

Introduction

Terry Draper, PE, PMP

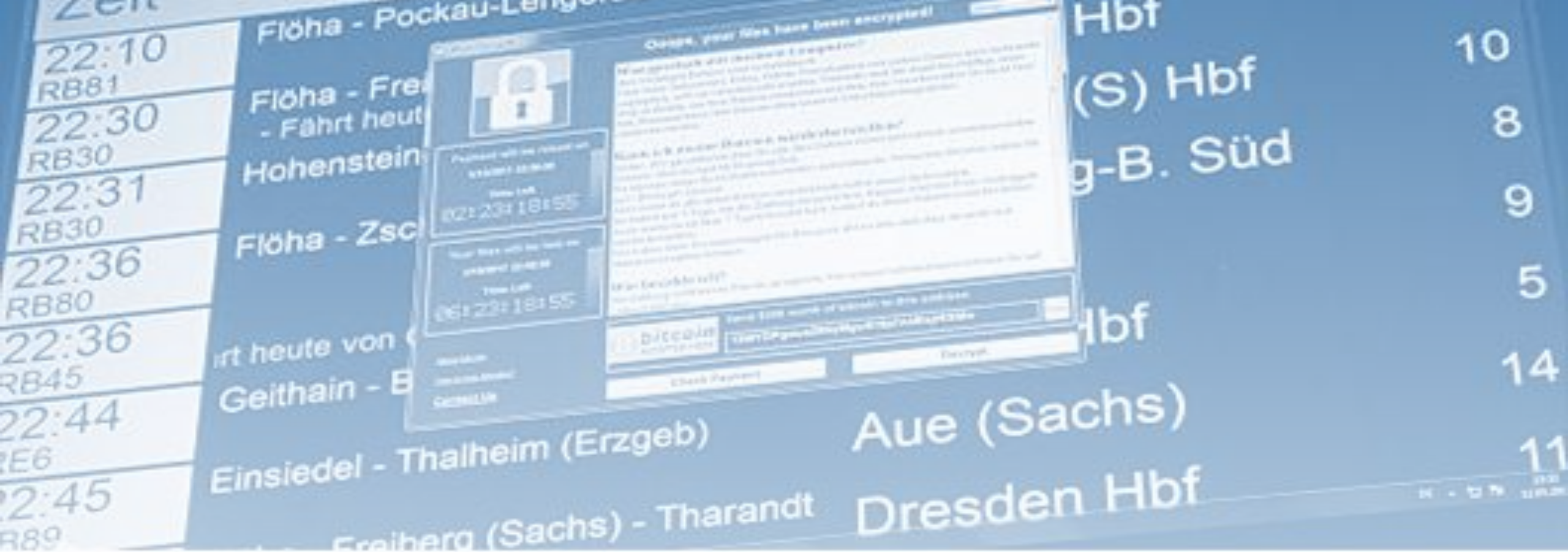
Jeff Coulson, MMSc, P.ENG, PMP

Cybersecurity Background and EMA Experience

- Water Utility Vulnerability Assessments – RAM-W (Post 9/11)
- Wastewater Utility Vulnerability Assessments – Initial VSAT (NACWA)
- WERF/WRF Project – “Security Measures for Computerized and Automated Systems at Wastewater/Water Utilities”: Developed CS2SAT (precursor to DHS CSET)
- AWWA Project – Process Control System Security Guidance Tool
- WRF Project – “Considerations for Security and Communications for Intelligent Water Systems”
- AWWA Project – PCS Security Guidance Tool Training and Tool Update
- OT/IT security assessments to address current threats and vulnerabilities including NIST guide to ICS security and above tools

Agenda

1. Challenges of Cybersecurity Assessments
2. Assessment Methodology
3. Starting an Assessment
4. Sustainability and Summary
5. Next Workshops
6. Questions



P. Goetzelt | AFP | Getty Images

A window announcing the encryption of data including a requirement to pay appears on an electronic [illegible] on May 12, 2017. A fast-moving wave of cyberattacks swept the globe, apparently exploiting a flaw exposed in documents leaked from the US National Security Agency.

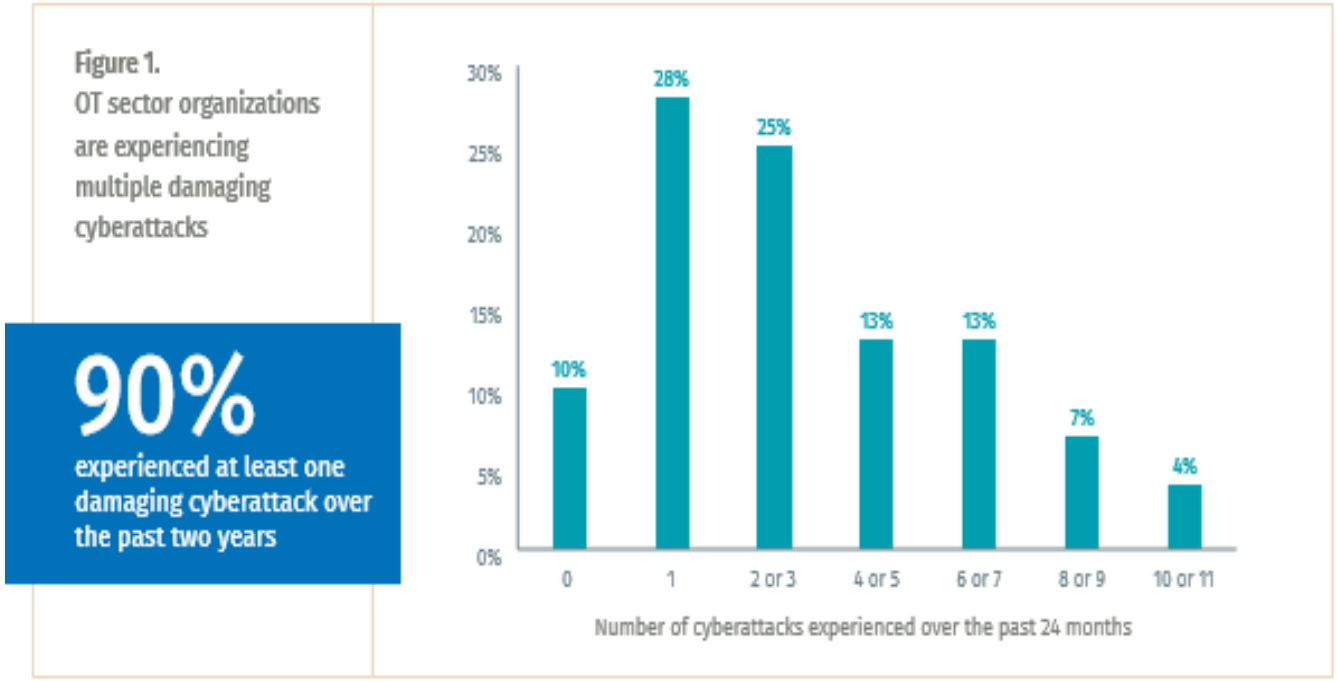
1. Challenges of Cybersecurity Assessments

Cybersecurity Threats Are Real and Damaging

What are threats?

- Cyber-terrorists
- Cyber-spies
- Cyber-thieves
- Cyber-warriors
- Cyber-hacktivists

- Current or former employees:
  - knowingly
  - unknowingly



Source: Ponemon Institute, “Cybersecurity in Operational Technology” March 2019

Ransomware Attacks Can Be Costly

- WannaCry – NHS (Britain) – Over $100M
- NotPetya, Merck - $915M[1] , Maersk - $200 to $300M[2]
- SamSam – Atlanta – $2.6M[3] to $17M[4]
- RobinHood – Baltimore – over $18M[5]
- Riviera Beach, FL – $600K Ransom and over $1M in HW and services[6]

P. Goetzelt | AFP | Getty Images

A window announcing the encryption of data including a requirement to pay appears on an electronic timetable display at the railway station in Chemnitz, eastern Germany, on May 12, 2017. A fast-moving wave of cyberattacks swept the globe, apparently exploiting a flaw exposed in documents leaked from the US National Security Agency.

1. FiercePharma, "Merck has hardened its defenses against cyberattacks like the one last year that cost it nearly $1B", Eric Palmer, Jun 28, 2018
2. Forbes, "NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million", Lee Mathews, Aug 16, 2017
3. Wired, "Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare", Lily Hay Newman, April 23, 2018
4. Atlanta Constitution Journal, "CONFIDENTIAL REPORT: Atlanta's cyber attack could cost taxpayers $17 million", Stephen Deere, Aug 1, 2018
5. Baltimore Sun, "Baltimore estimates cost of ransomware attack at $18.2 million as government begins to restore email accounts", Ian Duncan, May 30, 2019
6. Washington Post, "Florida city will pay hackers $600,000 to get its computer systems back", Rachael Siegel, June 20, 2019

AWIA Has Cybersecurity-Related Requirements

PL #115-270 - Sec. 1433(a)(1)(A) The RRA is an assessment of the risks to and resilience of the community water system including:

- electronic, computer, or other automated systems (including the security of such systems) which are utilized by the water system
- the monitoring practices of the system
- the financial infrastructure of the system
- the operation and maintenance of the system
- *may include an evaluation of capital and operational needs for risk and resilience management for the system*

Cybersecurity Assessments Require an Organization, Practice and Technology Approach

O	P	T
Knowledge spread across the organization, not centralized	Difficult to self-assess and document faults in own practices, documents and systems	IT and OT present a large amount of different assets to assess
Need IT & OT resources	Policies may not be in place or may be dated	Different tools are needed to assess systems

Cybersecurity Assessment Challenges

IT and OT

- There is not always a clean line between IT and OT systems and responsibilities
- IT and OT staff may share responsibilities and closely coordinate security and protection tasks and responses
  - IT and OT staff and support may also be fully separated
- Interfaces, integrations, and remote access cross IT and OT; responsibilities on both sides may not be clearly defined
- Incident response planning – are IT and OT aligned?

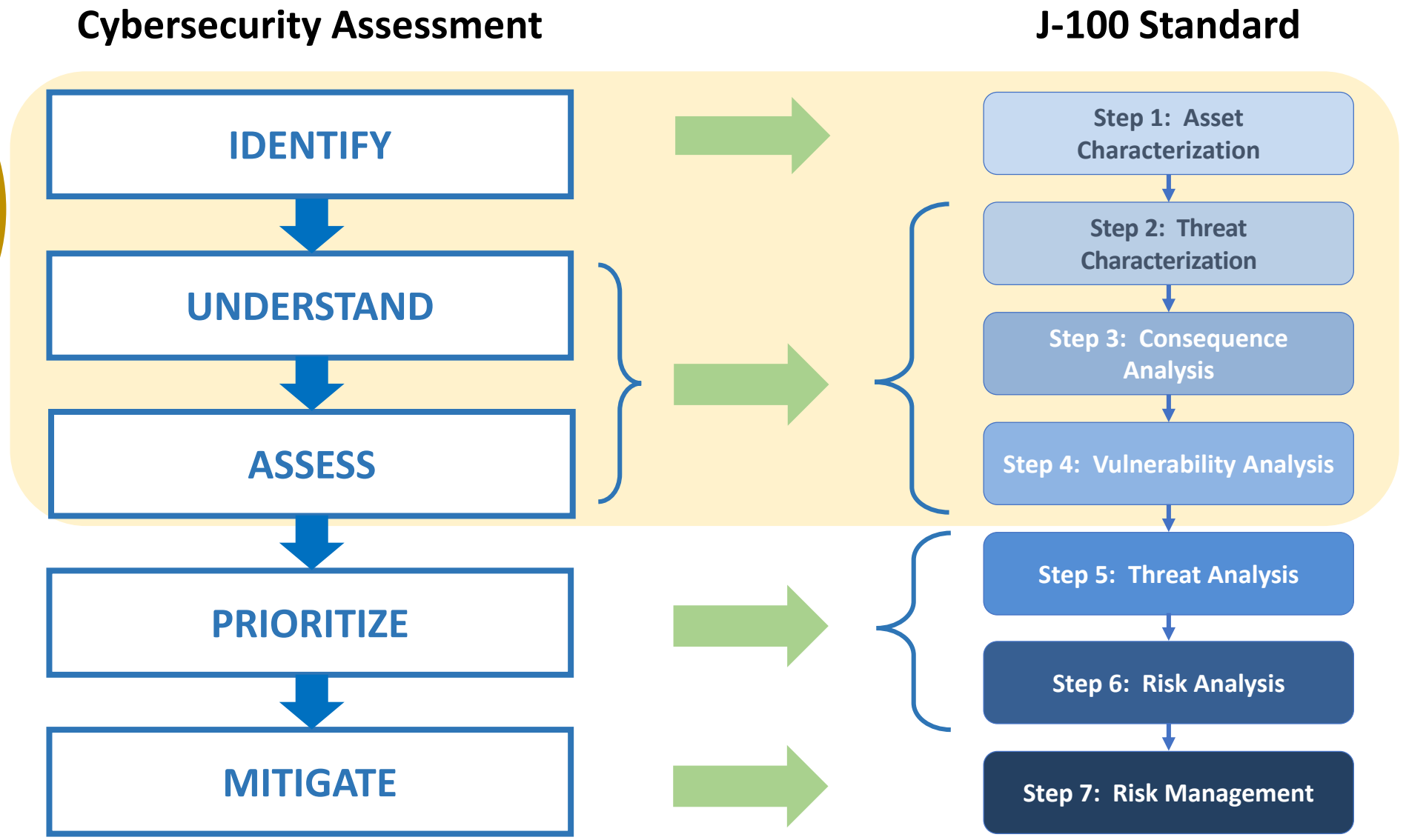
Challenge: OT Differs from IT

- PLC and control system technologies require different controls, protections, and maintenance
- IT policies and Practices may not be in place or enforced on OT systems
- Assessment of IT System (Business Systems) may not include OT
  - OT may be assumed to be isolated
  - Connections may be in place for Reporting, Data Transfer (USB) and Patching
  - Internal audits and external vendors may not be familiar with OT, miss items
- OT networks may not follow IT standards

2. Assessment Methodology

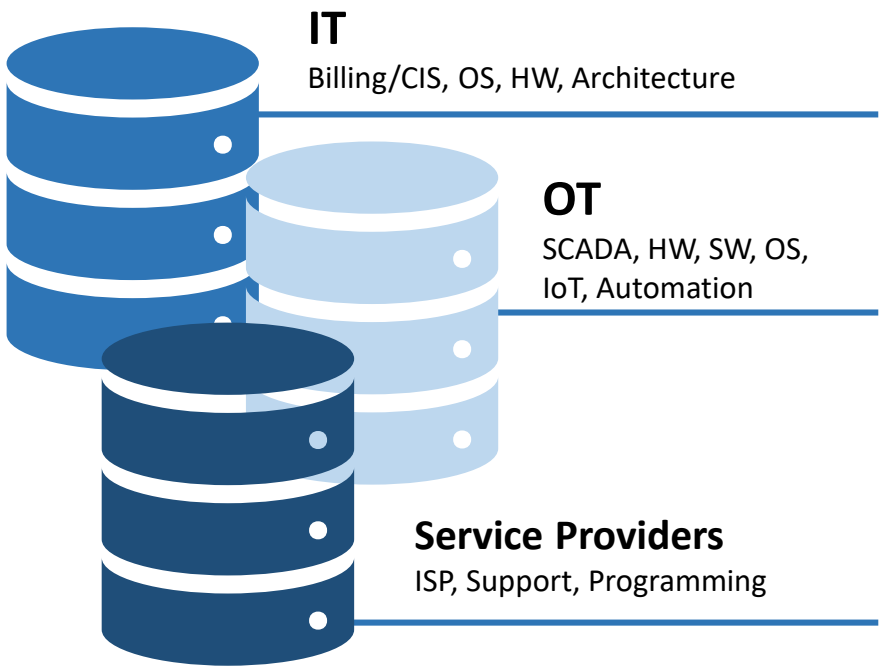
Assessment Methodology Aligns With J-100

We will focus on the **Identify**, **Understand** and **Assess** portion of the process

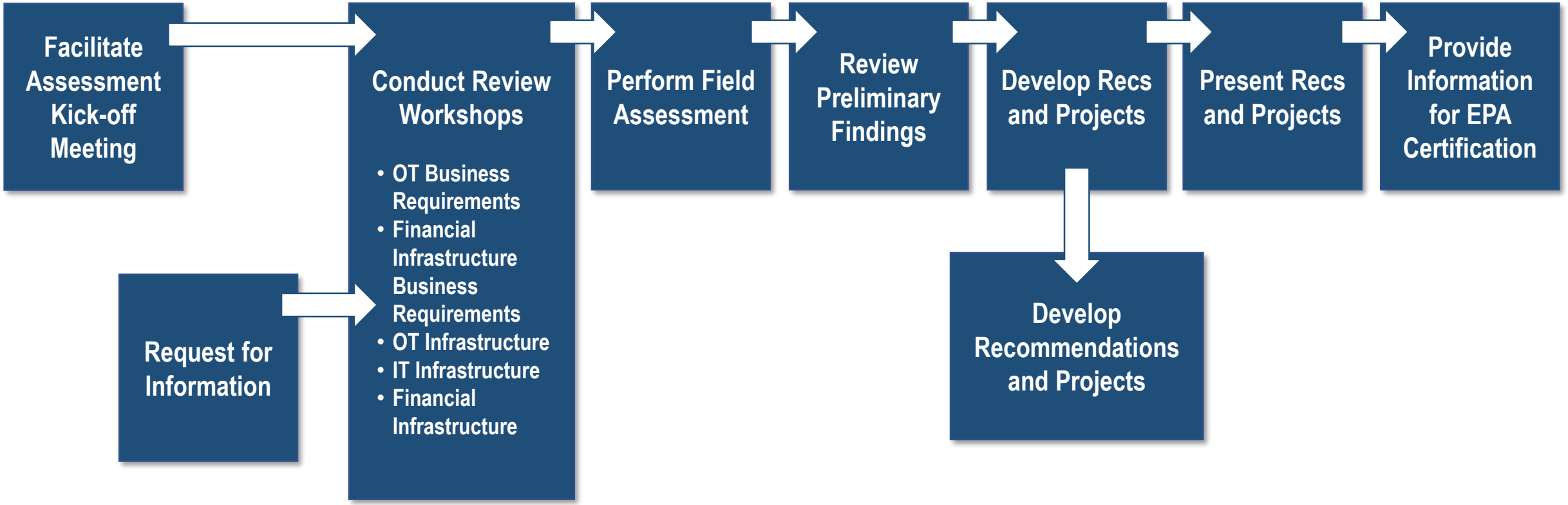


Comprehensive Approach for Assessment

- Assessment needs to identify how systems are used to determine what controls are needed
- Need participation and input from staff across the organization and with key partners



Comprehensive Approach for Assessment



Work closely with Utility staff, across the organization

Complete a bench audit to maximize workshop effectiveness

Include IT, Field and Process staff in workshops and interviews

Field assessments and system scanning

Workshops

- Client can use the AWWA Cybersecurity Guidance Tool for a pre-work activity, or this can be done in the workshops
- Assessment is a combination of data analysis, interviews and system scanning
  - Gather data, Interview staff, determine usage
- Knowing how the system is used, controls are identified; this can then be applied to what is scanned

Tasks

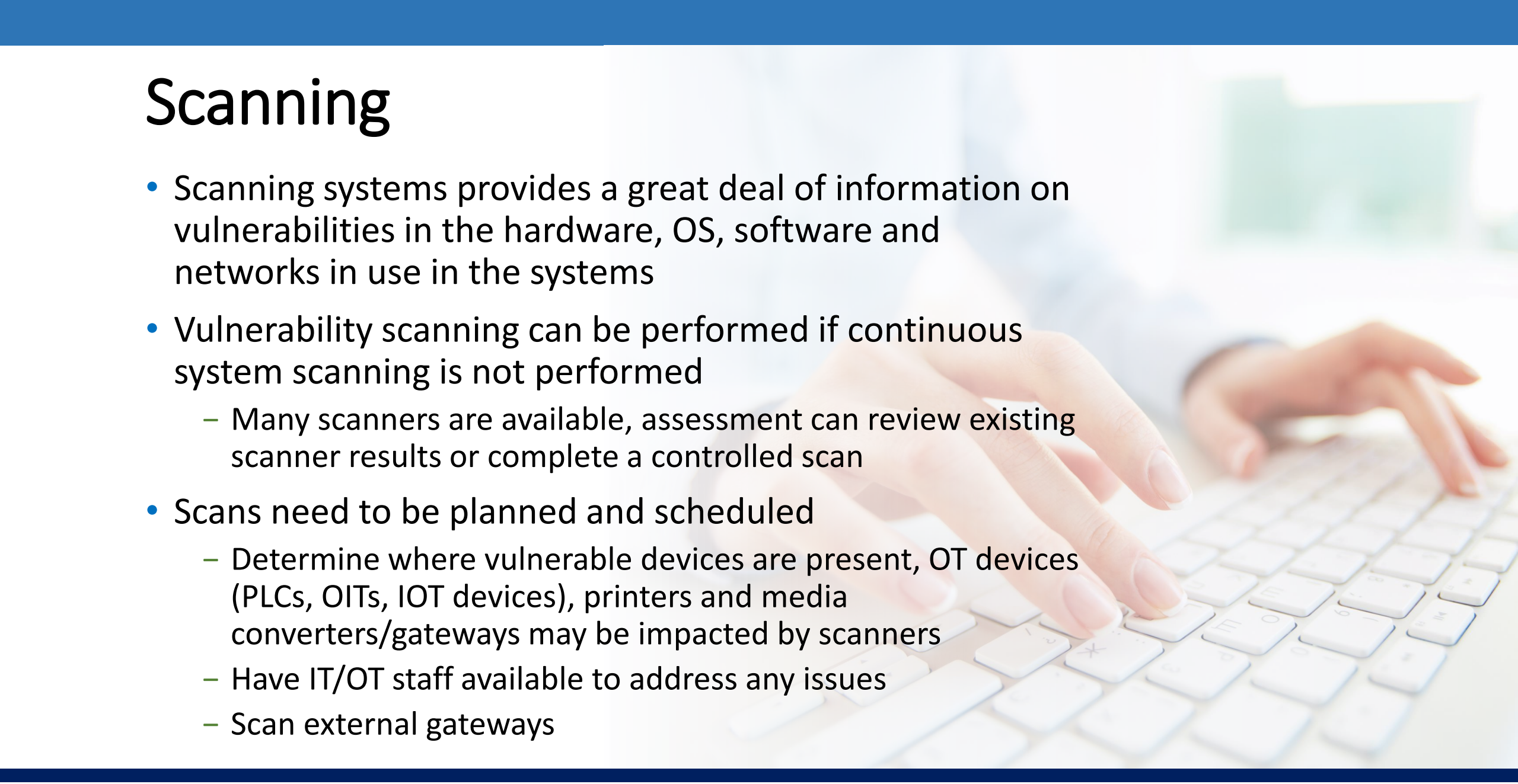
- ✓ Interviews with Stakeholders, identify goals and discuss schedule
- ✓ Request for Information
- ✓ Technology Workshop
- ✓ Operations Workshop
- ✓ System Maintenance Workshop
- ✓ Scanning
- ✓ Report development

Several Tools Can Be Used for Assessments

- VSAT & AWWA J-100 Standard (non-cybersecurity specific)
- AWWA Cybersecurity Guidance Tool
- Cybersecurity Evaluation Tool (DHS-CSET)
- NIST Standards
  - 800-82
  - 800-53
  - Cybersecurity Framework (CSF)
- Vulnerability scanners

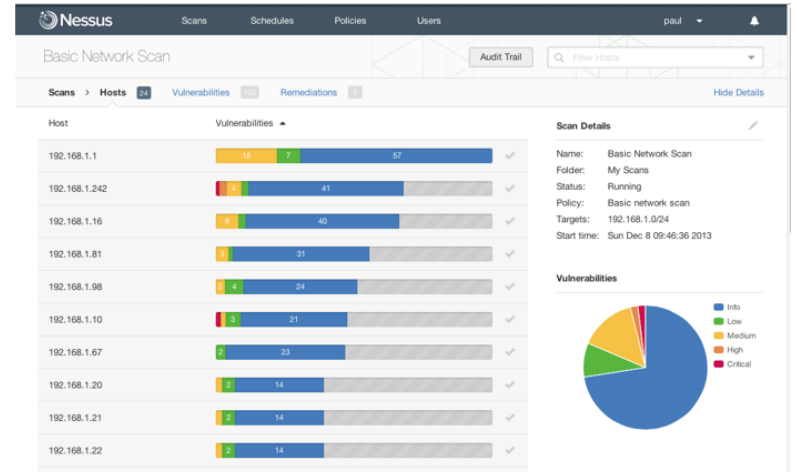
Scanning

- Scanning systems provides a great deal of information on vulnerabilities in the hardware, OS, software and networks in use in the systems
- Vulnerability scanning can be performed if continuous system scanning is not performed
  - Many scanners are available, assessment can review existing scanner results or complete a controlled scan
- Scans need to be planned and scheduled
  - Determine where vulnerable devices are present, OT devices (PLCs, OITs, IOT devices), printers and media converters/gateways may be impacted by scanners
  - Have IT/OT staff available to address any issues
  - Scan external gateways



Additional Field Testing

- Scanning systems will identify all connected assets, may identify unauthorized equipment and undocumented connections, investigate
- Scanning will not expose all vulnerabilities, many devices have default passwords, test these
- Test access to Wi-Fi networks, guest access, what is the area that is covered?
- Are modems still in use? What security is in place?
- Look at remote access and external facing systems in greater detail



3. Starting an Assessment

Getting Started

Look at assessments that have been completed in the past, are they still valid?

- Have systems been updated or changed
- Are new systems in place?
- Have staff adopted poor security practices?

The Assessment

- Develop an Assessment Plan
  - Include staff from across the organization in the discussions
  - Include service provider and third-party info
  - Be inclusive, need to identify where there are practice and system problems
- Plan for staff involvement in workshops
- Prepare documentation for assessment
- Assess controls against current practices
- Plan scanning and scan systems to discover vulnerabilities

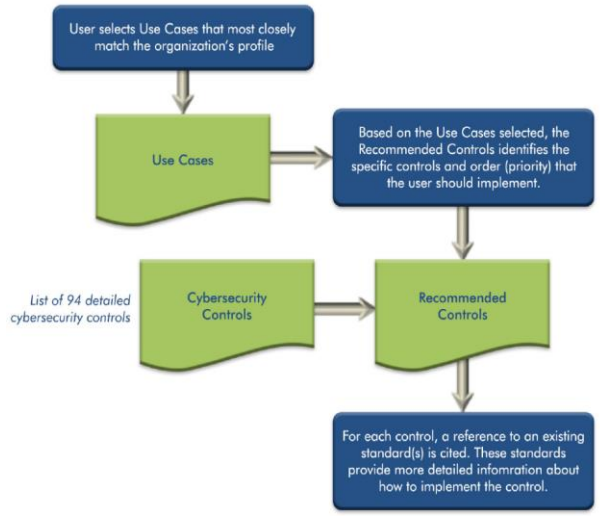
Document List

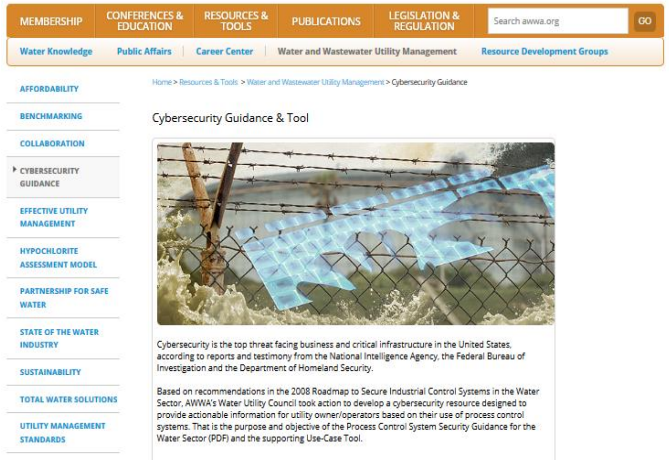
- ✓ OT Architecture
- ✓ IT Systems Architecture
- ✓ IP Lists
- ✓ Policies
- ✓ Service Level Agreements and third-party contracts

Getting Started

Complete a short self assessment

- Use the AWWA Guidance Tool or CSET Tool for OT systems
- Assess use of the Finance Infrastructure systems through business drivers
- Determine what controls are needed for the systems
- Are there gaps in what controls you have?
- Can they be fully identified and assessed internally?
  - If no look to define or request an assessment scope





The Assessment

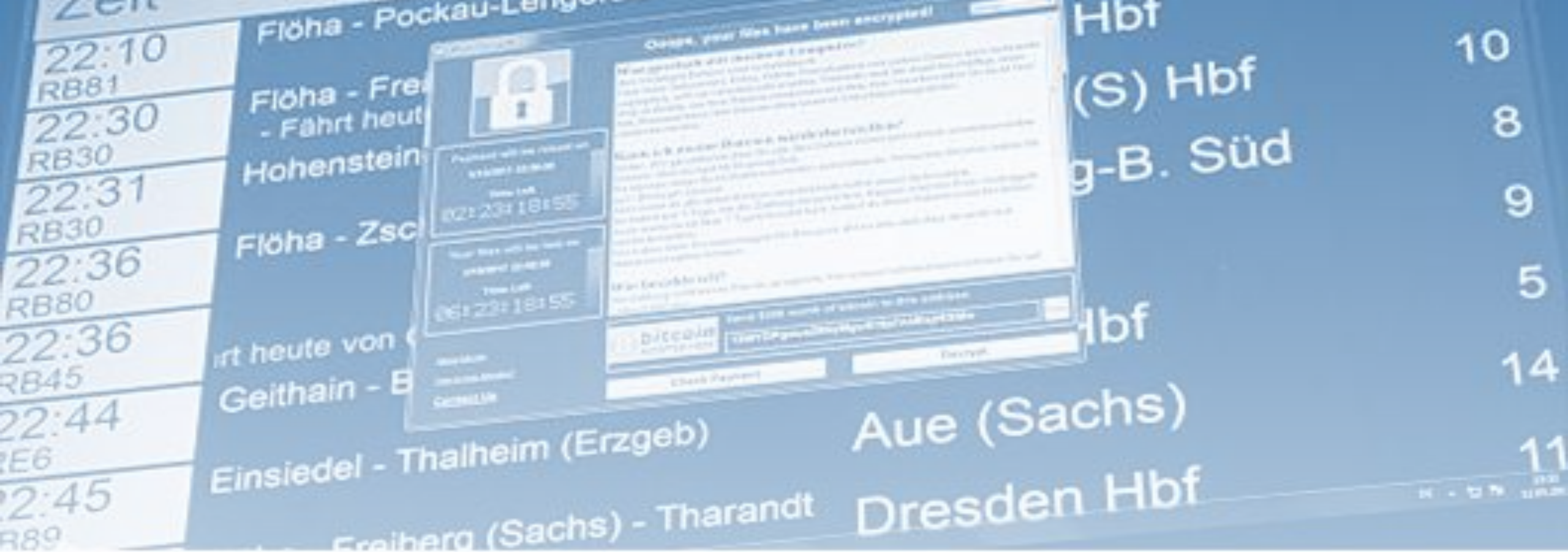
The assessment is quick, 3-6 months for most organizations

Staff involvement is intense at the workshops, but minimal overall

Be prepared to implement quick wins

Be ready to re-assess for changes, a new system, regulatory or practice change, not just a calendar event

Cybersecurity Assessment can be done independently or as part of the larger J100 methodology for the AWIA requirements

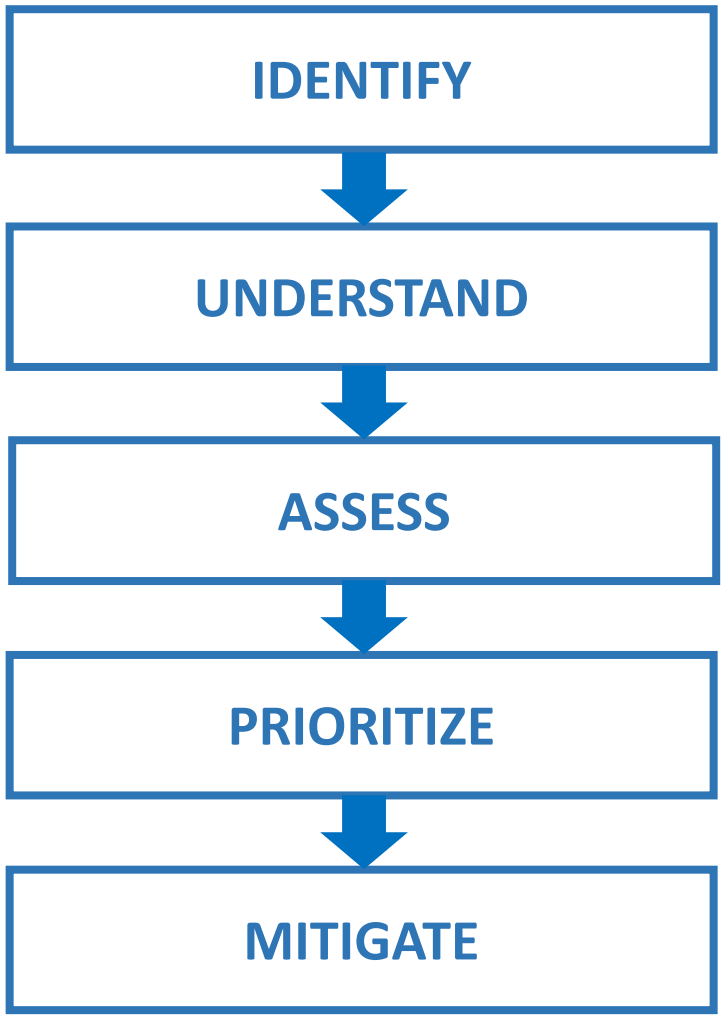


P. Goetzelt | AFP | Getty Images

A window announcing the encryption of data including a requirement to pay appears on an electronic [illegible] eastern Germany, on May 12, 2017. A fast-moving wave of cyberattacks swept the globe, apparently exploiting a flaw exposed in documents leaked from the US National Security Agency.

4. Sustainability and Summary

Assessment Yields Key Deliverables



RRA Is basis for improvement plan

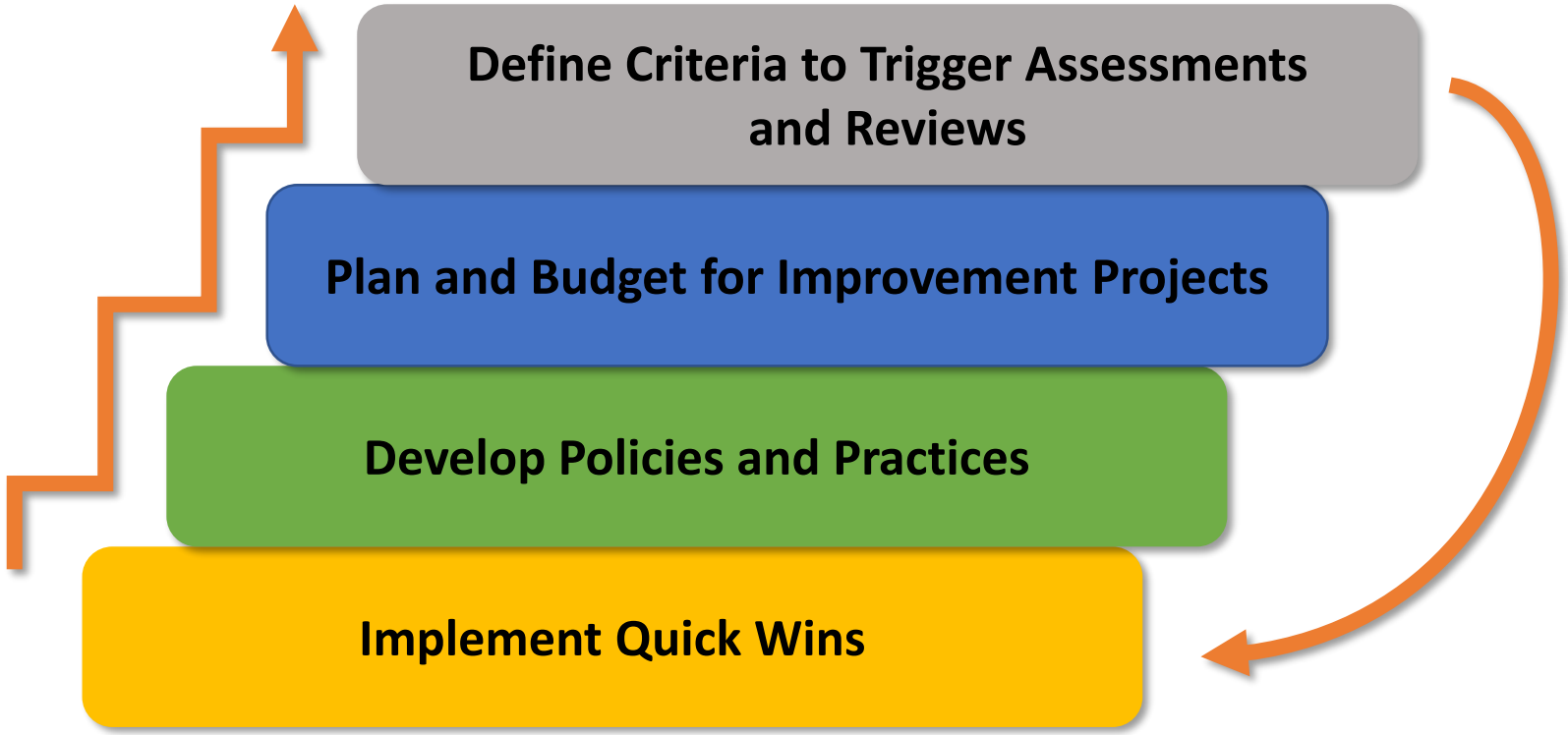
- Immediate risk mitigation
- Update of previous OT/IT Plans
- Longer-term improvements become part of ERP

Risk & Resiliency Assessment (RRA)

Risk Mitigation & Improvement Plan

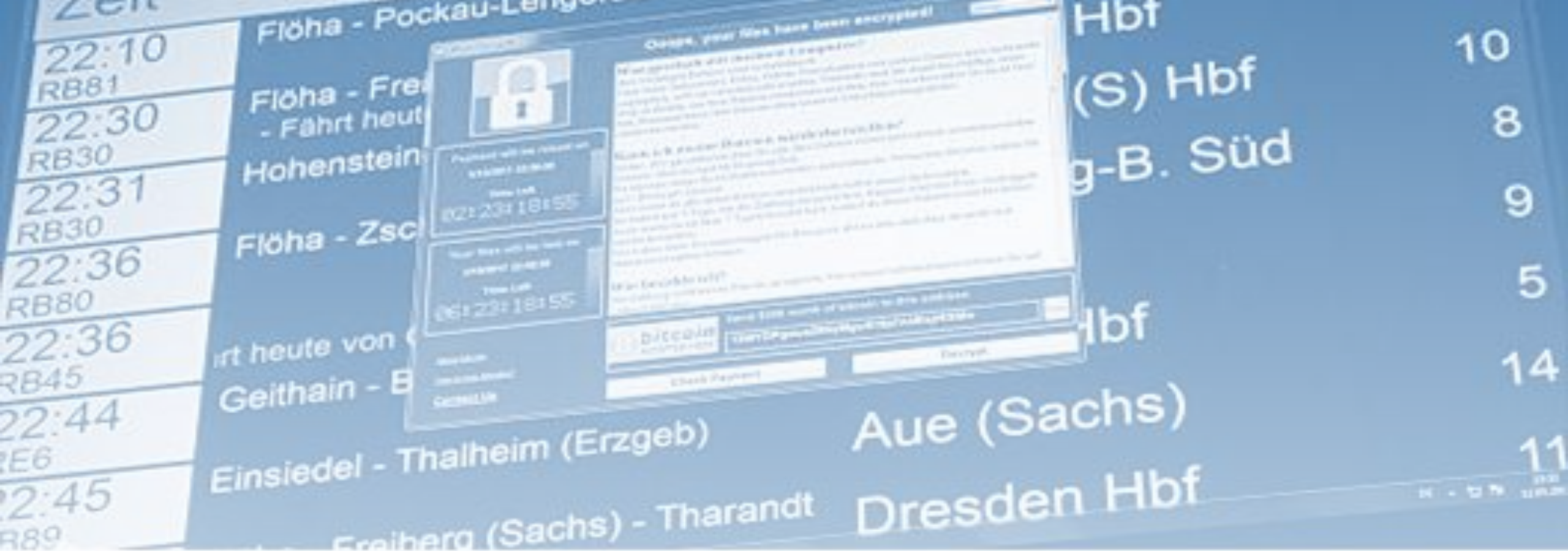
Emergency Response Plan (ERP)

On-going Vigilance



Summary

- It is easy to get started, create a Plan with staff across the organization and external parties
- Commit to the assessment and implement quick wins
- Develop Policies and Practices to inform, train and manage the human part of the organization
- Include Cybersecurity requirements in systems design and implementation
- Include longer-term projects in CIP and budgets
- This is an ongoing exercise, update policies and re-assess when threats or systems change



P. Goetzelt | AFP | Getty Images

A window announcing the encryption of data including a requirement to pay appears on an electronic ... ay station in Chemnitz, eastern Germany, on May 12, 2017. A fast-moving wave of cyberattacks swept the globe, apparently exploiting a flaw exposed in documents leaked from the US National Security Agency.

5. Next Webinars

Future Cyber Assessment Webinars

- Webinar 2 - Process Control and SCADA System Risks – August 20
  - Focus on the Operation Technology Risks, Assessment Tools and Outcomes

- Webinar 3 - Business System Risks – September 18
  - Focus on the Information Technology Risks, Assessment Tools and Outcomes

Register: waterisac.org/events

6. Questions

Contact

Jeff Coulson, EMA
jcoulson@ema-inc.com
651-628-5091

Terry Draper, EMA
tdraper@ema-inc.com
651-628-5014

Bob Reilly, EMA
breilly@ema-inc.com
407-786-5374

Additional RRA Webinar Series

Water Sector Risk and Resilience Assessments:

A WaterISAC Webinar Series

- August 27, September 11, and October 2, 2019

- Register at waterisac.org/events.

Other Resources

waterisac.org/awia

Thank You

Contact

Jeff Coulson, EMA
jcoulson@ema-inc.com
651-628-5091

Terry Draper, EMA
tdraper@ema-inc.com
651-628-5014

Bob Reilly, EMA
breilly@ema-inc.com
407-786-5374

Michael Arceneaux
Managing Director
arceneaux@waterisac.org

Charles Egli
Lead Analyst
egli@waterisac.org

1-866-H2O-ISAC