DHS Stakeholder Engagement Infrastructure Resilience (SECIR) Resource Brief

ICS Cybersecurity 101

Rick Gardner
Cybersecurity Advisor
Region VIII (UT, CO, MT, WY, ND, SD)
Cybersecurity and Infrastructure Agency (CISA)
Office of Cybersecurity and Communications (CS&C)
Cell: 801-822-1216
richard.gardner@hq.dhs.gov
Mission:

To provide direct coordination, outreach, and regional support in order to protect cyber components essential to the sustainability, preparedness, and protection of the Nation’s Critical Infrastructure and Key Resources (CIKR) and State, Local, Tribal, and Territorial (SLTT) governments.

Priorities:

• Protection & Sustainment of Critical Infrastructure
• Information Sharing
• Incident Response Support
CSAs assists the public and private sectors secure its networks and focuses on organizations in the following 16 critical infrastructure sectors.

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
  - Election Infrastructure
- Health Care & Public Health
- Information Technology
- Nuclear Reactors, Materials, & Waste
- Transportation Systems
  - Water / Wastewater Systems
Protected Critical Infrastructure Information (PCII)

The DHS Protected Critical Infrastructure Information (PCII) Program is an information protection program that enhances information sharing between the private sector and the government. The DHS and other federal, state and local analysts use PCII to analyze and secure critical infrastructure and protected systems, identify vulnerabilities and develop risk assessments, and enhance recovery preparedness measures.

If the information submitted satisfies the requirements of the CII Act of 2002, it is protected from:

- The Freedom of Information Act (FOIA)
- State and local disclosure laws
- Use in civil litigation

PCII cannot be used for regulatory purposes and can only be accessed in accordance with strict safeguarding and handling requirements. PCII may be accessed by federal, state or local government employees and their contractors who meet the requirements of the PCII Program standard access policy.

Before accessing PCII, these individuals must:

- Complete training on the proper handling and safeguarding of PCII
- Have homeland security responsibilities
- Have a need-to-know the specific information
- Sign a non-disclosure agreement (non-federal employees only)
- Be certified by the PCII Program Manager or PCII Officer (contractors only)
Regions (24 CSA’s) / +9FY19 /+22FY20
Cybersecurity Assessments

- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)
- Cyber Tabletop Exercise (CTTX)
- Phishing Campaign Assessment (PCA)
- Cyber Hygiene/Vulnerability Scanning (CYHY)
- Validated Architecture Design Review (VADR)
- Risk & Vulnerability Assessment (RVA)
Cyber Resilience Review (CRR)

- **Purpose:** The CRR is an assessment intended to evaluate an organization’s operational resilience and cybersecurity practices of its critical services.

- **Delivery:** The CRR can be
  - Facilitated
  - Self-administered

  CRR Self-Assessment Package is available on the C-Cubed Voluntary Program website.

- Helps public and private sector partners understand and measure cyber security capabilities as they relate to operational resilience and cyber risk.

- Based on the CERT ® Resilience Management Model (CERT® RMM))

  The CRR provides organizations with a no-cost method to assess their cybersecurity postures and measure against the NIST CSF.
**External Dependency Management (EDM)**

- **Overview:** In 2016, DHS launched the External Dependencies Management (EDM) Assessment, focusing specifically on ensuring the protection and sustainment of services and assets that are dependent on the actions of third-party entities.

- **Background:** External Dependencies Management is a domain covered by the CRR. However, EDM and associated issues (e.g., supply-chain management, vendor management) are not addressed at a comprehensive level within the CRR, resulting in the creation of a separate assessment.

- **Linkages to CRR:** Despite operating at a more granular level than the CRR, the EDM Assessment borrows heavily from the CRR’s methodological architecture and scoring system but remains a DHS-facilitated assessment.

The EDM Assessment provides stakeholders with a more in-depth examination of risks associated with their third-party entities.
External Dependency Management (EDM)

To provide the organization with an understandable and useful structure for the evaluation, the EDM Assessment is divided into three distinct areas (domains):

1. **RELATIONSHIP FORMATION** – how the organization considers third party risks, selects external entities, and forms relationships with them so that risk is managed from the start

2. **RELATIONSHIP MANAGEMENT AND GOVERNANCE** – how the organization manages ongoing relationships with external entities to support and strengthen its critical services at a managed level of risk and cost

3. **SERVICE PROTECTION AND SUSTAINMENT** – how the organization plans for, anticipates, and manages disruption or incidents related to external entities
Validated Architecture Design Review (VADR)

Overview:
The Validated Architecture Design Review (VADR) is an assessment based on Federal and industry standards, guidelines, and best practices. Assessments can be conducted on Information Technology (IT) or Operational Technology (OT) infrastructures (ICS-SCADA).

Assessment Objectives:
• Reduce risk to the Nation’s Critical Infrastructure components
• Analyze systems based on **standards, guidelines, and best practices**
• Ensure effective **defense-in-depth** strategies
• Provide findings and practical mitigations for improving operational maturity and enhancing cybersecurity posture
Validated Architecture Design Review (VADR)

ICS-CERT's assessment team works interactively with your IT and operations personnel to focus on **three key areas:**

- **Evaluation of Architecture**
  - An in-depth review and evaluation of the network design, configuration, and inter-connectivity to internal and external systems focused on defensive strategies

- **Analysis of Network Traffic**
  - Utilizes a combination of open source and commercial tools to identify anomalous communication which could indicate suspicious activity or misconfiguration

- **Systems Log Review and Analysis**
  - Detailed review of system settings and activity to determine the susceptibility to potential attacks and baseline normal behavior to find anomalies
Cyber Hygiene (CH)

Assess Internet accessible systems for known vulnerabilities and configuration errors

Work with organization to proactively mitigate threats and risks to systems

Activities include:

• Network Mapping
  - Identify public IP address space
  - Identify hosts that are active on IP address space
  - Determine the O/S and Services running
  - Re-run scans to determine any changes
  - Graphically represent address space on a map

• Network Vulnerability & Configuration Scanning
  - Identify network vulnerabilities and weakness
Cyber Hygiene (CH) - FAQ

• **How frequently will my Agency be scanned?**
The frequency of the scans is up to your Agency. In addition to on-demand scans, NCATS would like to conduct quarterly, monthly, or weekly scans.

• **Will my Agency have a decision in scan scheduling?**
Once we receive the signed authorization letter, we assign a Technical POC to work with your agency POC to validate /determine your public IP space and identify the frequency and time frames the scanning may occur.

• **Will my Agency be expected to "white list" DHS scanning IPs?**
Your Agency is not required or expected to "white list" the DHS scanning range, although the results will be more thorough if you do. The choice is entirely up to your agency. A couple of days prior to scanning activity we send notification letters (email) to US-CERT and to any identified Agency SOCs explaining the activity and identifying the source IP range so they will be prepared.

• **What level of access to the reports and data will my Agency have?**
In addition to the report we prepare your Agency will have full access to all data and findings produced by our tools.
WATER / WASTEWATER SYSTEMS
This brief is intended to provide an overview of control systems, applicable cyber threats, and ways to protect them.

Learn why control systems are susceptible to cyber-type attacks, what vulnerabilities are specific to the control system environment, and the effects of cyber attacks on control systems.
Evolution – Panel Based Controls

- Push Buttons
- Single Loop Controls
- Stand Alone
- No Networks
- No Communication

From a cyber security standpoint this system is ‘isolated’
Evolution – Legacy Equipment

- Proprietary Networks
- Proprietary OS
- No Ethernet
- No Intranet connections
- “Security by Obscurity”

From a cyber security standpoint this system is
‘exploitable – but not a trivial task’
From a cyber security standpoint this system is
‘a huge challenge – readily exploitable’
Water System Interdependencies
What is the Emerging Risk?

- No authentication amongst ‘isolated’ components
- Modbus/ICCP/DNP3 fully published and open for review

Pre-existing attack landscape
What is one thing wrong with the network?
U.S. Water Utility

- **Event:** January 2011, U.S. water utility reports a security breach of its remote terminal service machine that allows access to the SCADA system

- **Impact:** Remote logon service for after hours access was not responding, but no impacts to the SCADA network were observed

- **Specifics:** 7,463 incidents of malware traffic were communicating with the utility’s computers. Only 77 were unique known malware (spam, brute force ssh, virus/worms) originating from 57 compromised hosts. Analysis concluded that the observed activity was crimeware related.

**Lessons learned:**
- Secure remote access with solutions such as VPN or two-factor authentication
- Leverage the static nature of a control system to look for anomalies
- Prepare and utilize an incident response plan
**Event:** Residents of a rural town experienced loss of water pressure.

**Impact:** Approximately 10,000 residents were without water.

**Specifics:** Utility operator updated its HMI OS (Windows) with a direct connection to the Internet and evidence points to a virus infecting the SCADA system; causing it to crash.

The ICS was outdated, not supported by the vendor, and not patched to current updates. It also lacked a firewall between the business and control networks.

**Lessons learned:**
- Utilize DMZ to ensure isolation from business side and Internet
- Keep systems patched
- Establish and enforce sound security policies
Ransomware Masked as Rockwell Update

**Event:** Ransomware masquerades as a control system update. Real life “wolf in sheep’s clothing”.

**Impact:** Trick employees into copying malware onto a system and then require a ransom to rectify the problem.

**Specifics:** “Rockwell Automation has learned about the existence of a malicious file called ‘Allenbradleyupdate.zip’ that is being distributed on the Internet. This is NOT an official update from Rockwell Automation, and we have been informed that this file contains a type of ransomware malware that, if successfully installed and launched, may compromise the victim’s computer.”

Lessons learned:
- Obtain software/firmware updates directly from the vendor
- Develop, deploy and test backup and recovery procedures
Harrisburg Pennsylvania Water System

- **Event:** Foreign hacker penetrated security at a water filtering plant

- **Impact:** The intruder planted malicious software that was capable of affecting the plant’s water treatment operations

- **Specifics:** The infection occurred through the Internet and did not seem to be an attack that directly targeted the control system

**Lessons learned:**
- Secure remote computers
- Defense-in-depth strategies, firewalls and intrusion detection systems
- Critical patches and antivirus needs to be applied and updated regularly
Maroochy Waste Water

- **Event:** More than 750,000 gallons of untreated sewage intentionally released into parks, rivers, and hotel grounds

- **Impact:** Loss of marine life, public health jeopardized, $200,000 in cleanup and monitoring costs

- **Specifics:** Used commercially available radios and stolen SCADA software to make laptop appear as a pumping station

**Lessons learned:**
- Suspend all access after terminations
- Investigate anomalous system behavior
- Secure radio and wireless transmissions
ICS Incident – Multiple Sectors

- Multiple spear-phishing incidents in recent months involving major U.S. corporations: Banking, Energy, Nuclear, Water
  - Emails are designed to look like intra-office traffic including company-specific topics of concern
  - Actors use company websites and social media to do reconnaissance
  - Emails spoof actual account user names
  - Main Goal: data exfiltration for industrial espionage and trade secrets

Lessons learned:
- Threat actors are becoming more sophisticated
- Common attack vector to gain a foothold
- Employee education and training
USB Drives

- **Event:** An employee attended an industry event and used an instructor’s USB to download presentation materials. The USB was unknowingly infected with the Mariposa botnet.

- **Impact:** Over 100 computers at the employee’s organization were infected.

- **Specifics:** When the employee returned to work and plugged the laptop into the network, the virus quickly spread.

**Lessons learned:**
- Implement policies for analysis and use of USBs
- Isolate critical networks and implement controls for connections involving removable media
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>What are you doing to eliminate input validation errors such as buffer</td>
<td>Implementing secure coding practices, protocol authentication checks,</td>
</tr>
<tr>
<td>overflows, OS and SQL command injection, and cross-site scripting?</td>
<td>and security reviews of deployed IT software?</td>
</tr>
<tr>
<td>Have you addressed code quality issues such as implementing secure</td>
<td>Protocol authentication checks, and security reviews of deployed IT</td>
</tr>
<tr>
<td>coding practices, protocol authentication checks, and security reviews</td>
<td>software?</td>
</tr>
<tr>
<td>of deployed IT software?</td>
<td>Do you test operating system patches?</td>
</tr>
<tr>
<td>Does your system have any hard-coded passwords?</td>
<td>Do you provide security patches for your ICS application as vulnerabilities are discovered?</td>
</tr>
<tr>
<td>Do you run your servers as a process or a service?</td>
<td>Do you have security level agreements with your vendors and third-party</td>
</tr>
<tr>
<td>Have you incorporated the latest versions of third-party software?</td>
<td>partners?</td>
</tr>
<tr>
<td>Do you test operating system patches?</td>
<td></td>
</tr>
<tr>
<td>Do you provide security patches for your ICS application as vulnerabilities are discovered?</td>
<td></td>
</tr>
<tr>
<td>Do you have security level agreements with your vendors and third-party partners?</td>
<td></td>
</tr>
</tbody>
</table>
Water ISAC

- The U.S. water and wastewater sector’s leading national associations and research foundations established the Water Information Sharing and Analysis Center (WaterISAC) in 2002, in coordination with the U.S. Environmental Protection Agency.

- WaterISAC is the designated information sharing and operations arm of the Water Sector Coordinating Council.

- WaterISAC is a comprehensive and targeted single point source for data, facts, case studies, and analysis on water security and threats from intentional contamination, terrorism and cyber crime. WaterISAC also provides analysis and resources to support response, mitigation, and resilience initiatives.
ICS Training Opportunities

ICS-CERT Virtual Learning Portal (VLP)

- Virtual & Instructor Led Training
- No Cost

Courses:

- Introduction to Control Systems Cybersecurity (101) - 8 hrs
- Intermediate Cybersecurity for Industrial Control Systems (201) - 8 hrs
- Intermediate Cybersecurity for Industrial Control Systems (202) - 8 hrs
- ICS Cybersecurity (301) - 5 days

https://ics-cert-training.inl.gov/learn
DHS Contact Information

Rick Gardner
Cyber Security Advisor, Region VIII
UT, CO, MT, WY, ND, SD
Office of Cybersecurity & Communications
U.S. Department of Homeland Security

Email: Richard.gardner@hq.dhs.gov
Mobile: (801) 822-1216