GERRIE
AUTOMATION GROUP

A Comprehensive Resource Guide for Securing Critical Infrastructure

Rockwell Automation

Table of Contents

Introduction

Critical Infrastructure organizations are undergoing digital transformation, digitizing processes and adopting Internet of Things (IoT) technology to improve efficiency and reliability. The resulting connectivity of operational technology (OT) to the internet and the convergence between OT and IT have created extreme efficiencies, as well as new vulnerabilities and exposure to cybersecurity threats.

As the U.S. National Security Agency (NSA) and the Cybersecurity & Infrastructure Security Agency (CISA) noted in a joint alert, cyber actors are demonstrating "their continued willingness to conduct malicious cyber activity against Critical Infrastructure by exploiting internet-accessible OT assets." And these cyberattacks are growing in their size, sophistication, and prevalence.

Many of the principles for defending your IT environment apply to industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems and other OT. But securing OT has additional complexities and considerations.

We've created this resource guide with more than 80 useful reference links, categorized and described, to shortcut your learning about the evolving Critical Infrastructure threat landscape, the modern industrial cybersecurity practices used for defense, and steps to formulating your own plans and strategies.

Growing Critical Infrastructure Threats

In the past two years, attacks on Critical Infrastructure (CI) providers like Colonial Pipeline, a Florida water treatment facility, and Israeli water and wastewater facilities have demonstrated the growing vulnerability of the Critical Infrastructure sector. Those are not isolated incidents; among 179 CI organizations surveyed in 2021, 83% reported experiencing OT cybersecurity breaches in the past 36 months.

The consequences of these cyberattacks can extend far beyond costs and disruption. Gartner predicts that by 2025, cyberattackers will weaponize OT to harm people.

READ THE REPORT

SECTION 1

What Critical Infrastructure Security Leaders Should Know

Many ICS systems are easily accessible to hackers, as this investigation by the research-based publication Cybernews.com shows. The threat landscape continues to evolve. Gartner points out that as OT systems are changing, so are the threat actors' tactics and techniques.

Hackers remain the top source of ICS network intrusion, a SANS survey of 480 cybersecurity practitioners found. Weak security protocols and lack of standardization contribute to IoT attacks in the Critical Infrastructure sector, notes this article published by the World Economic Forum.

Top Threats Impacting Critical Infrastructure

- **Malware.** The UK National Cyber Security Centre provides an explanation of how malware works, along with examples and defense strategies.
- **Advance persistent threats (APTs).** Get technical details from CISA and advice from the NSA on mitigation strategies.
- **Insider threats.** The U.S. National Counterintelligence and Security Center provides guidelines for Critical Infrastructure entities and CISA offers a guide for implementing an insider threat program for Critical Infrastructure.
- **Nation-state attacks.** Review examples in this CISA article about threats originating from China.
- **Ransomware.** Watch a virtual discussion with CISA's acting director and the McCrary Institute for Cyber and Critical Infrastructure Security, and read CISA's overall guide to ransomware for IT professionals.

Cybersecurity Fundamentals and Best Practices

Government agencies, industry-specific organizations, and professional cybersecurity services firms offer guidance around creating and implementing the right cybersecurity program. Below are several articles and websites outlining best practices around Critical Infrastructure defense.

One of the core cybersecurity frameworks recognized worldwide is from the U.S. National Institute of Standards and Technology (NIST). NIST's SP 800-82, "Guide to Industrial Controls Systems (ICS) Security" includes an overview of ICS, covering security fundamentals such as risk management and assessment, security architecture, and the application of IT controls to ICS, as well steps for responding and recovering from security incidents.

These resources offer 'at a glance' best practices:

- **Tips and Tactics for Control Systems Cybersecurity.** A NIST infographic with quick tips and fundamental steps to take.
- **Cybersecurity Practices for Industrial Control Systems.** A high-level but comprehensive, two-page overview from CISA and U.S. Department of Energy (DOE).
- **ICS Cybersecurity for the C Level** — a two-page guide to help facilitate cybersecurity conversations with the C suite and other stakeholders.

For a deeper dive into the current threat landscape and on getting started with a cybersecurity plan, read CISA's "A Guide to Critical Infrastructure Security and Resilience." Additionally, the WaterISAC's comprehensive "15 Cybersecurity Fundamentals for Water and Wastewater Utilities" discusses best practices that are applicable across the Critical Infrastructure sector, including:

- Performing asset inventories
- Enforcing user access controls
- Creating a cybersecurity culture
- Securing the supply chain
- Implementing threat detection and monitoring

SECTION 2

Regulatory Considerations

As threat actors increasingly target Critical Infrastructure providers and facilities, governments are mandating better security and resilience. The United States in particular has been very active in this arena, continuously tightening regulations. For example, the July 2021 Presidential memorandum on improving CIS cybersecurity aims to increase the federal government's collaboration with the private sector to improve defenses.

While the initiative itself is voluntary, new standards will emerge from it for managing risk and security. Critical Infrastructure organizat' leaders should watch the developments closely to understand how the changes may drive future regulatory compliance.

Regulatory resources:

- **CISA overview.** A review of objectives and the nine areas that CISA and NIST will focus on as a result of the memorandum.
- **NIST update.** NIST will update its SP 800-82 (Guide to Industrial Control Systems Security); the update is a result of the memorandum.
- **Expert insights.** Read commentary from a legal firm on implications.
- **Networks and Information Systems (NIS) Directive.** The European Union's directive on supervision of critical sectors. For an analysis of the directive's implications for Critical Infrastructure sectors and how it maps to other standards, such as NIST and ATT&CK, read the SANS white paper, "ICS within the NIS Directive should be ATT&CK®ed" (requires free membership).

SECTION 3

Cybersecurity Frameworks

Cybersecurity frameworks offer roadmaps for managing Critical Infrastructure risks and implementing risk mitigation strategies. While several industry frameworks can be adapted to Critical Infrastructure, Rockwell Automation recommends the NIST Cybersecurity Framework (CSF), which includes best practices for comprehensive cybersecurity protection based on five core functions: Identify, Protect, Detect, Respond and Recover. The framework allows for flexibility, and you can customize activities based on your individual needs and environment.

The NIST CSF, which was originally created specifically to address Critical Infrastructure, has become a standard across industries. U.S. federal agencies have been required to apply the framework to federal information systems since 2017. Government contractors that need to follow specific requirements such as NIST 800-53 can also map to NIST CSF to demonstrate compliance.

Resources to help with NIST CSF implementation:

- NIST Interagency Report 8170 discusses approaches to CSF for federal agencies. While targeting the report to federal users, NIST expects private companies using CSF to benefit as well.
- Sector-specific implementation guides that can be broadly applied to Critical Infrastructure include those from DOE for energy, Department of Homeland Security for transportation systems and CISA for dams.

Additional Frameworks and Models

- **IIoT Consortium's** Security Maturity Model**.** The model was designed for IoT systems owners, integrators, decision makers and other stakeholders (see additional insights in the practitioner's guide).
- **MITRE ATT&CK.** Developed by federally-funded research, MITRE is widely used by security practitioners. ATT&CK is a matrix and a curated knowledge base of adversary tactics and techniques based on real-world observations; a recently added section specific for industrial control systems can help security teams with tactical execution. CISA also uses ATT&CK in some of its threat advisories — see this October 2021 alert to water and wastewater system operators as an example.
- **ISO 27000 and IEC 62443.** This series of standards developed by the International Standard Organization (ISO) and the International Electrotechnical Commission (IEC) guide risk management and security. Many businesses pursue ISO/IEC certification to prove their compliance with security practices. IEC 62443 was developed to provide flexibility for organizations to look at cybersecurity and risk throughout the supply chain vs. strictly at the asset owner level.
- **UK's Cyber Assessment Framework (CAF).** Developed by the UK National Cyber Security Center (NCSC) for securing the Critical Infrastructure sector, this set of 14 principles cover areas such as asset management, supply chain, staff awareness and training, and response and recovery planning.
- **Cybersecurity Maturity Capability Model (C2M2).** This Department of Energy model was developed in cooperation with the private sector to address IT/OT cybersecurity practices and is applicable across Critical Infrastructure verticals. C2M2 includes more than 300 cybersecurity practices categorized into 10 domains, such as threat and vulnerability management, risk assessment, workforce management and cybersecurity architecture.

SECTION 4

Core Functions of the NIST Cybersecurity Framework

Here are several useful resources to explore along the NIST categories of Identify, Protect, Detect, Respond and Recover.

Identify

This domain pertains to understanding your cybersecurity risks, including their business context and your available resources.

- **OT Cybersecurity Quick Assessment.** Developed by Rockwell, this tool provides a quick read on cybersecurity readiness and gaps, and offers recommendations and benchmarking data from peer organizations by industry, size and region.
- **IIoT/IoT scanning tools** — a list of three publicly available tools for discovering internet-facing ICS devices and tips for using the tools; CISA also offers detailed information on each of the tools here.
- **Cyber Security Evaluation Tool (CSET).** Free desktop software offered by CISA to evaluate control system networks' cybersecurity.
- **Guide for Conducting Risk Assessments.** NIST Publication 800-30, geared to federal information systems but applicable to private sector.
- **Insider risk assessment.** A downloadable self-assessment kit from CISA.

For organizations that would like more comprehensive services, Rockwell offers network asset identification and scanning, along with ongoing asset inventory monitoring to help identify security risks on an ongoing basis. Learn more.

Protect

This domain focuses on developing and implementing safeguards such as data security, identity management and access controls, the right architecture, product security and more, including such needs as staff awareness and training.

- **ISC-CERT advisories.** A list of various vendors' common vulnerabilities and exposures (CVEs); also see additional CVE repositories from NIST and MITRE.
- **Identity and access management (IAM).** This introduction to IAM by the NCSC includes a section on OT.
- **Defending Against Software Supply Chain Attacks.** A white paper by CISA for software developers and their clients.
- **Protecting internet-facing services.** An article by the NCSC, geared to Critical Infrastructure operators.
- **Videoconferencing security for Critical Infrastructure entities.** Recommended practices from CISA.

Detect

In this function, continuous monitoring processes are implemented to detect cybersecurity incidents.

- **Cyber hygiene assessments**. A list of free services, such as vulnerability scanning, phishing testing, and penetration testing, offered by CISA to Critical Infrastructure organizations.
- **Defense-in-depth overview**. Although developed for the nuclear sector by CISA, this infographic has quick insights applicable across the board.
- **SOC buyers guide**. For organizations considering outsourcing their security operations center, this NCSC guide provides an in-depth SOC overview and tips.

For organizations that would like more comprehensive services, Rockwell offers anomaly and threat detection services, as well as strategic partnerships with global providers like Claroty and Cisco. Learn more.

Respond and Recover

The last two NIST CSF domains focus on taking action during cybersecurity events to stop breach attempts from succeeding and then spreading, and then on restoring operations back to normal levels. These categories use of attack attempts to improve insight and resilience.

- **Incident communication templates**. A variety of downloadable forms from SANS.
- **Tabletop exercises**. Kits for cybersecurity response scenarios from CISA.
- **Incident response playbook**. While targeted to public power entities, this DOE playbook can be adapted to any Critical Infrastructure vertical.
- **Incident response planning**. A step-by-step guide from NCSC. Additionally, see the useful guide on building an incident response team.
- **Preparing for a cyber incident**. An introductory guide from the U.S. Secret Service Cyber Investigations, based on the NIST CSF.
- **Real-world example**. An interesting article about the city of New Orleans, following its own incident response plan and thwarting a ransomware attack.

SECTION 5

Designing a Secure OT Architecture

One of the nine CISA focus areas mentioned above is architecture and design. Integrating cybersecurity features such as network segmentation, firewalls and Demilitarized Zone (DMZ) separation into your architecture reduces your attack surface, makes intrusion more difficult and improves detection and response.

Zero Trust is one of many approaches that can contribute to a better cybersecurity architecture, built on the idea that no user, connection or request can be trusted automatically without being continuously and dynamically authenticated and authorized. CISA now considers Zero Trust an enhanced objective in response to the presidential mandate to improve Critical Infrastructure cybersecurity.

Cybersecurity architecture resources:

- **Secure Architecture Design.** An interactive page from CISA with definitions and documentation for ICS components, ranging from wireless access points to web applications servers.
- **Design Principles and Operational Technology.** NCSC recommendations on designing secure OT systems.
- **Security architecture anti-patterns.** An NCSC white paper for design patterns to avoid, applicable to OT.
- **Zero Trust Maturity Model.** A draft document from CISA designed to help federal agencies implement a Zero Trust approach. (Check here for updates.)
- **CNI Systems Design: Secure Remote Access**. A comprehensive NCSC article for the Critical Infrastructure sector, important during pandemic operations.
- **NIST Publication 800-207.** Comprehensive discussion of the Zero Trust strategy and deployment variations.
- **Rockwell and John Kindervag on Zero Trust in OT.** Hear the latest insights around Zero Trust in OT from Rockwell and John Kindervag, originator of the Zero Trust approach.

Cybersecurity grants in US infrastructure bill

In November 2021, U.S. Congress enacted a far-reaching infrastructure spending bill, H.R. 3684, Infrastructure Investment and Job Act. (See Sections 40121-40127, 50113 and Title VI, Sections 70611-70612 for interesting cybersecurity content).

As part of the act, DHS will fund grants for cybersecurity improvements in Critical Infrastructure organizations. Public services such as water/wastewater and electric utilities, oil & gas processors, transportation and healthcare facilities - as well as private organizations in 16 CISA-identified industries – are targeted to be eligible for grant support.

What will grants cover?

Guidelines are expected to be published in 2022, but grants will likely cover a wide range of investments around hardening IT, OT and ICS security defenses across the five NIST categories of Identify, Protect, Detect, Respond and Recover.

Organizations can begin defining and documenting their cybersecurity needs now to help accelerate plan development and submission, if such a plan does not already exist.

Rockwell Automation has developed a free cybersecurity plan template and checklist you can download as a first step toward building a formal cybersecurity plan, suitable for submission for DHS grant funding. Need additional help on insight? Contact Rockwell.

SECTION 6

Industry-Level Resources

The industry-specific resources below have useful information and advice that any Critical Infrastructure organization can adapt. Here are some examples:

- **Pipelines cyber risk mitigation**. Quick overview from CISA.
- **Water sector best practices**. A list of cybersecurity resources from the EPA.
- **Checklist for incident response**. Developed by EPA for the water sector.
- **IoT security best practices**. A detailed guide on industrial IoT for smart manufacturing by EU's Agency for Cybersecurity (ENISA).
- **Cybersecurity risk in the water sector**. A white paper from the American Water Works Association.

Cybersecurity in Critical Infrastructure is evolving quickly. To stay ahead of threats, security leaders need to watch emerging trends, regulatory developments and industry changes on an ongoing basis. One great final set of resources are CISA's email lists, with options for receiving ongoing news, alerts, tips and more.

If you're looking for expert industrial security advice and guidance on how to best secure Critical Infrastructure, Rockwell can help. We can assess, design, implement and manage a variety project-based or ongoing managed services solutions. With 100+ years supporting organizations in the heart of industry, our global footprint, industrial-strength SOC capabilities and hands-on-keyboard cybersecurity teams, we can ensure your production operations are extremely well-protected.

Learn more, then contact us today to schedule an expert consultation.

Connect with us.

rockwellautomation.com — expanding **human possibility**®

AMERICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
EUROPE/MIDDLE EAST/AFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
ASIA PACIFIC: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication GMSN-WP005A-EN-P - June 2022