Setting up a Comprehensive and Enduring OT Cybersecurity Program

AIT
Applied Integrated Technologies

Robert Sadler
Larry Jaffe
Applied Integrated Technologies
August 2, 2022

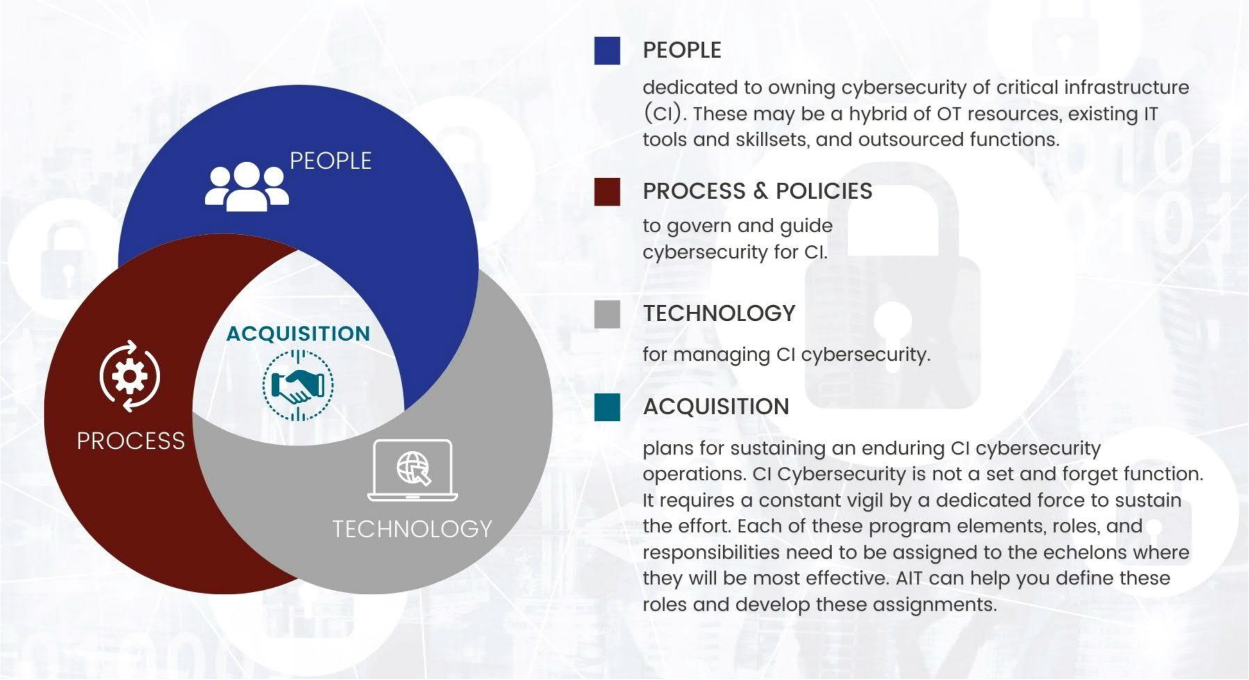
Contents

Introduction

Establishing an Operational Technology (OT) Cybersecurity functional organization is imperative in securing critical infrastructure and reducing risk. A lack of ownership of OT cybersecurity leads to critical infrastructure incidents and impacts. Actively managing OT cybersecurity identifies accountability and demonstrates good faith effort by the company to protect assets for employees, customers, neighbors, shareholders, and insurance.

Successfully managing OT cybersecurity is dependent on how it is implemented within the organization. The OT cybersecurity organization belongs within Plant Operations and not as an IT function. This whitepaper proposes a model OT cybersecurity organization. It describes what it might look like: its people, processes, technologies, and the acquisition required to sustain it. AIT stands ready to support industry in their efforts to understand, acknowledge, plan, and execute an Enduring Cybersecurity Program.

AIT's approach to OT cybersecurity is to develop a comprehensive and enduring cybersecurity program scaled to meet the specific needs of your organization. This effort primarily involves overlaying a cybersecurity function across multiple OT functions in a cohesive and cooperative structure. Most importantly, this new cybersecurity function leverages existing IT tools and skillsets where it makes sense to do so[i]. Key components of such a program typically include:



PEOPLE

dedicated to owning cybersecurity of critical infrastructure (CI). These may be a hybrid of OT resources, existing IT tools and skillsets, and outsourced functions.

PROCESS & POLICIES

to govern and guide cybersecurity for CI.

TECHNOLOGY

for managing CI cybersecurity.

ACQUISITION

plans for sustaining an enduring CI cybersecurity operations. CI Cybersecurity is not a set and forget function. It requires a constant vigil by a dedicated force to sustain the effort. Each of these program elements, roles, and responsibilities need to be assigned to the echelons where they will be most effective. AIT can help you define these roles and develop these assignments.

Each of these program elements, roles, and responsibilities need to be assigned to the echelons (enterprise, region, or plant-level) where they will be most effective. AIT can help you define these roles and develop these assignments.

People

An OT cybersecurity organization should possess a few key skills and roles. These roles include managers, engineers, technicians, OT cybersecurity analysts, and cyber researchers.

Management should have knowledge of OT Plant operations and program management for OT and IT functions. They should also be able to communicate technically across organizations and manage incident responses.

Engineering personnel act as consultants to the OT operations and should be able to provide the engineering technical expertise on systems and all associated component architectures, operations, and functions. The engineers are responsible for designing and implementing cyber informed engineering for secure architectures and technologies. The technical staff should possess computer engineering degrees and computer science degrees with backgrounds in imbedded systems and industrial protocols. In addition to cybersecurity skills, personnel with backgrounds in instrumentation and controls would be helpful.

Technicians maintain the ICS equipment and systems. They are the field force for OT cyber operations for firmware updates, field observations, incident response, and assisting in recovery operations. They are responsible for the safe and secure operations of the ICS systems.

OT cybersecurity analysts provide the organization with an understanding of the threats and techniques of threat actors. They help drive the posture of OT cybersecurity. Key skills they require are:

- threat analysis methodologies
- cybersecurity best practices for OT and IT networks
- excellent written and oral communications
- ability to work with engineers, cyber researchers, and management regarding cybersecurity compliance and auditing

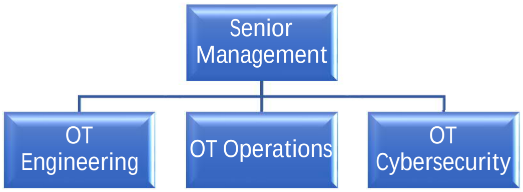
Cyber researchers liase with IT organizations and assist with pushing out cybersecurity policy, requirements, and regulations into the OT environment. Their knowledge and skills should include:

- industry cyber security standards, regulations, and guidelines
- conducting cyber assessments, including inventorying system hardware
- a background with computer forensics and incident response
- penetration testing
- the ability to work with cyber analysts and engineers in the course of their duties

With these five basic functional roles addressed in the OT cybersecurity organization, companies will find significant success in overcoming cyber threat and attack challenges. For additional reading on the resources needed to staff and manage an OT Cybersecurity organization refer to the joint publication between the Idaho State University and Idaho National Laboratory, “Building and Industrial Cybersecurity Workforce – A Managers Guide.”[ii]

Organization

OT Cybersecurity is not a set and forget function. It requires a constant vigil by a dedicated, scalable force to sustain the effort. Current OT maintenance operations are largely reactive in nature; therefore, OT cybersecurity cannot be a collateral duty assigned to existing staff. Currently this function either doesn’t exist or is very



limited in its implementation. How best to organize these skillsets may be unique to your organization, but our observations are that setting the OT cyber organization in parallel to operations and engineering works best.

Standing up an OT control system cybersecurity organization with clear ownership and tasking assigned to a dedicated staff can ensure the unique security and maintenance needs are met for the ICS environments.

Topic	IT	Control Systems
Availability	Reboots allowed for applying patches	Maintenance windows are few and far between
Consequences of Downtime / Outages	Data and production can typically be recovered.	Data often not reconstructable. Process restarts are highly disruptive
Endpoint Protection	Common and easy to deploy	Most OT components do not support endpoint protection
Technology Support Lifetime	3 to 4 year lifecycle	20+ year lifecycle
Physical Security of Assets	Offices and data centers are relatively easy to secure	Remote location of some assets make physical security more challenging.
Internet Access	Systems designed for internet access	Older systems were never intended to be internet attached

Table 1. Common differences between IT and OT

Processes

The OT cybersecurity organization should work closely with engineering, operations, and IT departments in support of control system assets and act as a bridge between systems engineering and IT. They should be responsible for setting OT cybersecurity policy, developing procedures, and executing cybersecurity processes such as:

IT vs OT

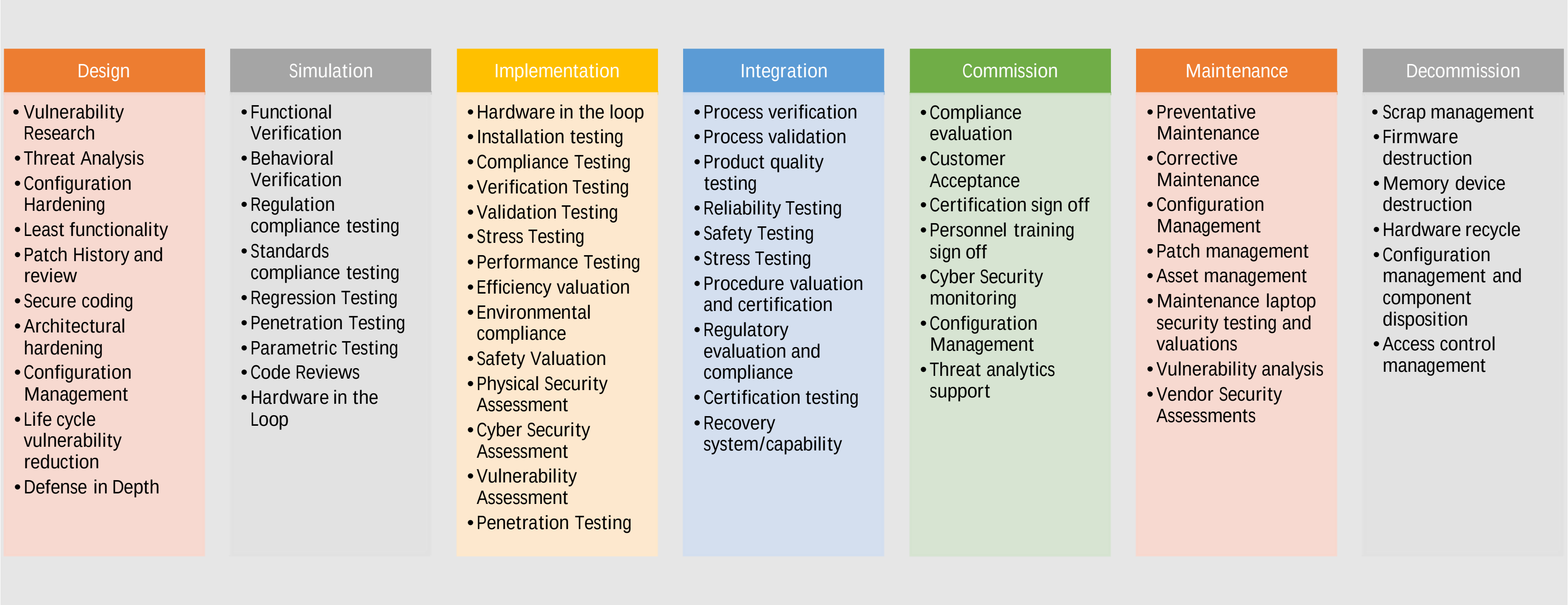
There are significant differences in duties and responsibilities between IT and OT organizations that often go unrecognized when trying to implement an OT function. OT cybersecurity should also not be the sole responsibility of an IT organization because of the unique nature of control systems as opposed to common IT systems. Control systems in general require an understanding of the physics behind the process and knowledge of many different embedded operating systems, numerous industrial communication protocols, and unique physical level interfaces. Control systems have the added requirement to be online 24x7 without maintenance windows for patching. Table 1 lists additional unique differences between IT and control systems.

- Assessing OT cybersecurity standards and requirements
- Conducting and coordinating incident response, intelligence analysis, and aiding in forensics
- Networking monitoring and intrusion detection
- Ensuring physical security controls on critical infrastructure equipment and spaces.

They will be an integrated team member in system design reviews and aid in equipment selections as lead consultants to engineering staff. They will handle coordinating and consulting with the IT department on system integration into OT networks.

The OT cybersecurity organization will be responsible for evaluating contractor control system cybersecurity awareness and establishing control system cybersecurity training for all relevant company personnel working on, with or around OT control systems.

OT Cybersecurity processes should cover OT Cybersecurity operational needs and be integrated into the engineering lifecycle of your industrial control systems. The chart below depicts mature integration of an OT cybersecurity program into the OT engineering and operations lifecycle.



Design

- Vulnerability Research
- Threat Analysis
- Configuration Hardening
- Least functionality
- Patch History and review
- Secure coding
- Architectural hardening
- Configuration Management
- Life cycle vulnerability reduction
- Defense in Depth

Simulation

- Functional Verification
- Behavioral Verification
- Regulation compliance testing
- Standards compliance testing
- Regression Testing
- Penetration Testing
- Parametric Testing
- Code Reviews
- Hardware in the Loop

Implementation

- Hardware in the loop
- Installation testing
- Compliance Testing
- Verification Testing
- Validation Testing
- Stress Testing
- Performance Testing
- Efficiency valuation
- Environmental compliance
- Safety Valuation
- Physical Security Assessment
- Cyber Security Assessment
- Vulnerability Assessment
- Penetration Testing

Integration

- Process verification
- Process validation
- Product quality testing
- Reliability Testing
- Safety Testing
- Stress Testing
- Procedure valuation and certification
- Regulatory evaluation and compliance
- Certification testing
- Recovery system/capability

Commission

- Compliance evaluation
- Customer Acceptance
- Certification sign off
- Personnel training sign off
- Cyber Security monitoring
- Configuration Management
- Threat analytics support

Maintenance

- Preventative Maintenance
- Corrective Maintenance
- Configuration Management
- Patch management
- Asset management
- Maintenance laptop security testing and valuations
- Vulnerability analysis
- Vendor Security Assessments

Decommission

- Scrap management
- Firmware destruction
- Memory device destruction
- Hardware recycle
- Configuration management and component disposition
- Access control management

Technology

Applying technology to OT cybersecurity requires a deep understanding of the control system, associated components, and technologies. In addition, it requires understanding how to integrate the latest available cybersecurity software and tools into an existing OT architecture.

Embedded operating systems and custom firmware predominate in OT systems, but are not typically found in commercial systems. The custom nature of the embedded OT systems and firmware make it difficult to integrate security into this environment.

Judicious application of cybersecurity technologies are key to successful risk reduction. There are a number of technologies available to amplify and automate the OT cybersecurity function. The chart below shows some of the functions where technologies can be applied.

AIT's Full-Spectrum OT Cybersecurity Solutions

IDENTIFY

- Asset Identification
- Asset Management
- Cyber Risk Assessment
- Penetration Testing
- Physical Security Assessment
- Policy Creation and Maintenance
- Regulatory Evaluation
- Risk Management & Program Metrics
- Third-party Risk Assessment
- Threat Analysis
- Vulnerability Assessment
- Vulnerability Research

PROTECT

- Access Control Management
- Configuration and Patch Management
- Configuration Hardening
- Cyber Commissioning
- Cyber Exercises
- Defense in Depth
- Mitigation and Remediation
- Product Evaluation
- RMF / NIST CSF
- Sandboxing / Simulation
- Secure System Design
- Strategic Planning
- Third Party Design Reviews
- Training
- Virtual Testbed

DETECT

- Continuous Cybersecurity Monitoring
- Site Inspections
- Threat Intelligence
- Auditing

RESPOND

- Case Management
- Continuity of Operations
- Evidence Collection
- Incident Response
- Incident Response Playbooks
- Integration with your Incident Response Teams
- Supplemental Incident Response Personnel

RECOVER

- Communications Planning
- Lessons Learned Improvements
- Recovery Kits
- Recovery Planning
- System Restoration or Recovery

AIT prides itself in providing the full spectrum of OT cybersecurity solutions. We stand at the ready to support and assist you in determining the optimal application of technology for your organization.

Acquisitions/Sustainment

An acquisition function should be developed and maintained to support OT Cybersecurity day-to-day operations. This will allow effective support infrastructure within the Plant Operations from which to implement and maintain current industry standards and regulations. The acquisition function should be responsible for logistics, research and development, and program sustainment. This may be integrated into existing acquisition organizations and budgets to sustain OT Cybersecurity operations. Acquisition is a critical function necessary to ensure an effective OT Cybersecurity program and maintain continuous monitoring of the security posture.

The acquisition function will be responsible for sustainment of a wide array of program assets and processes such as:

- Personnel and contractors
- Hardware
- Software
- Workforce development
- Intelligence resources
- Engineering
- Portable electronics
- Supply Chain
- Contracting Language
- Facilities
- Contractor auditing
- Equipment evaluation
- Software evaluation
- Contracting procedures and training development

AIT Tip regarding policies, standards and guidelines

CIS top 20 are a good baseline to start from. ISA/IEC 62443 is more sophisticated and industry oriented, and is being set as the cross-industry standard in Europe and Canada.

NIST 800-82 is a widely accepted standard in the USA and when combined with the NIST CSF is tailored to your situation.

If you are a DoD vendor, you may want to consider the CMMC standard being promulgated in 2022.

See AIT's 20 weeks to Better ICS Cybersecurity series on LinkedIn for 20 or so recommendations based on our assessment activities over the past three years.

Roadmap

While your industrial control system may watch over some highly scientific processes but setting up your enduring cybersecurity program doesn't have to be "rocket science." Here is AIT's recommended roadmap for building your program:

Step 1. Figure out the resources, structure, and governance of your OT cybersecurity function.

Step 2. Develop your policies, standards, and guidelines.

Step 3. Develop your incident response capability.

Step 4. Focus on compliance and making that process as simple as possible.

Step 5. Create metrics to manage your progress.

Step 6. Build cybersecurity into your workforce development program.

Conclusion

OT cybersecurity is a necessary function for reducing risk to your industrial control systems. However, OT Cybersecurity is not a set and forget function. It requires the constant vigil of an enduring program consisting of People, Processes, and Technology along with an acquisition component to sustain the effort.

Identifying the right people, with the right background, who are dedicated to critical infrastructure protection is crucial. Doing so will shortening the length of time for Plant Operations to mature a sustainable critical infrastructure protection program. Processes need to be developed and technology must be applied to simplify and automate cybersecurity functions. Finally, budgeting for sustainment of the OT cybersecurity program is necessary to ensure the program endures.

AIT is a small company and certified MBE that prides itself on talent and capability. Our CMAC division's sole focus is ICS critical infrastructure cybersecurity. We have a wealth of talent and skill in this area. Please contact AIT it you would like more information regarding our capabilities and services. Our mission is to ensure you can accomplish your business or mission needs by securing your critical infrastructure from cyber threats.

[i] This paper is written for mid-sized to large critical infrastructure owner/operators. Small owner/operators need a different approach. AIT will address that in another whitepaper.

[ii] Idaho State University, Idaho National Laboratory, "Building an Industrial Cybersecurity Workforce – A Managers Guide," 2021, URL: ICS_Workforce-ManagersGuide2021.pdf (inl.gov), last accessed 7/18/2022.