SANS SECURITY AWARENESS

Industrial Control Systems Cybersecurity Awareness Training

INTRODUCTION

With human involvement accounting for about 80% of compromises, managing human-related risks is as crucial as technological defenses. In the realm of Industrial Control Systems (ICS) and Operational Technology (OT), specific cybersecurity awareness is essential for protecting critical infrastructure.

This ICS cybersecurity awareness training poster equips engineers, operators, and leaders with the necessary knowledge and skills to deploy role-based, ICS-specific, short-course training modules. This training can be rolled out to their workforce as part of a new or existing cybersecurity program. The SANS ICS Security Awareness Training Modules foster a culture of cybersecurity and clearly delineate the distinction between IT and ICS/OT, enhancing safety and resilience and informing decision-making to ensure the continuous protection of vital engineering systems.

ICS SECURITY – THE HUMAN LAYER

A foundational layer of ICS defense in depth involves policies, procedures, and awareness. Awareness includes training that aligns with the culture of safety and ICS cybersecurity among operators, engineers, and leaders who are responsible and accountable for industrial operations.

Regardless of the role within an organization that utilizes industrial control systems and processes, everyone plays a crucial part in this layer of defense and approach to securing the critical infrastructure against cyber threats.

ICS/OT-DEDICATED SECURITY AWARENESS

ICS assets are often inaccurately compared to traditional IT assets. Unlike IT systems, ICS systems have unique missions, objectives, and incident impacts that involve specialized devices and industrial protocols. Adversaries targeting industrial control systems use distinct tactics to compromise safety, control, and physical assets.

While IT security focuses on digital data and the pillars of confidentiality, integrity, and availability, ICS/OT focuses on the safety of personnel and the systems that manage real-time engineering processes and physical actions. Mature critical infrastructure security programs incorporate dedicated ICS security awareness content, such as videos, posters, etc., beyond traditional IT security content.

Some key differences between IT and OT/ICS are:

ICSSSA_ICS418_1124
Poster created by Dean Parsons—co-author of SANS ICS418 course.

ics.sans.org

ICS SECURITY ESSENTIALS FOR LEADERS: SANS ICS418™ TRAINING

ICS security is an ever-changing field requiring practitioners to continually adapt defense strategies to meet new challenges and threats. To compound the issue, any security changes need to be thoroughly tested to maintain the safety and reliability of industrial operations.

Globally, "critical infrastructure" and "operators of essential services" represent hundreds of thousands—if not millions—of industrial organizations. Some of them are the lifelines to our modern society, like water, energy, food processing, and critical manufacturing—but every industrial facility deserves to know their process is secure and safe. With increased threats, new technology trends, and evolving workforce demands, it is vital for security managers in operational technology (OT) to be trained in techniques to defend their facilities and their teams.

The two-day ICS418 course fills the identified gap amongst leaders working across critical infrastructure and OT environments. It equips new or existing managers responsible for OT/ICS, or converged IT/OT cybersecurity. The course provides the experience and tools to address industry pressures to manage cyber risk to prioritize the business—as well as the safety and reliability of operations. ICS leaders will leave the course with a firm understanding of the drivers and constraints that exist in these cyber-physical environments and will obtain a nuanced understanding of how to manage the people, processes, and technologies throughout their organizations.

ICS SECURITY AWARENESS BENEFITS

- Offers 20+ live-recorded, instructor-led ICS modules
- Continuously updated by SANS-certified ICS field practitioners and subject-matter experts
- Driven by ICS threat intelligence and use-cases
- Ensures all employees understand their role in cybersecurity, regardless of position
- Educates administrative, leaders, and non-technical staff on their critical roles in protecting ICS
- Provides modular, computer-based training for flexible scheduling based on role
- Includes knowledge checks to enhance comprehension and retention
- Provides performance tracking, metrics, and reporting for improving maturity
- Short and flexible format for deployment
- Can be hosted on the SANS platform or your organization's learning management system
- SCORM and US Federal 508 compliant
- Option to brand with your logo

ICS AWARENESS IMPLEMENTATION STRATEGY

Those responsible for ICS/OT cybersecurity, such as managers and CSOs, must measure the participation and effectiveness of the ICS security awareness program. It is advantageous to ensure ICS security short-course training modules are mandatory for the key roles to enable effectiveness. Similar to mandatory on-site physical safety requirements, like personal protective equipment (PPE) and physical safety training, ICS/OT cybersecurity can be integrated into mandatory training as well, directly aligned with the physical safety culture requirements. Leverage knowledge checks to track progress by user and role. To start a deployment for ICS security awareness training, ICS risk leaders can apply the awareness, desire, knowledge, ability, and reinforcement (ADKAR) model, tailored for staff, operators, and facility management to highlight the importance of ICS security and establish a repeatable maturing program.

ADKAR

The ADKAR model is a behavioral change management framework consisting of awareness, desire, knowledge, ability, and reinforcement. In ICS/OT cybersecurity awareness, ADKAR helps by creating awareness of ICS/OT cybersecurity importance, fostering the desire to adopt best practices, providing necessary knowledge, ensuring the ability to apply it, and reinforcing these practices to maintain security over time that aligns to an existing physical safety culture. Applying ADKAR in this way builds a robust security culture in ICS/OT environments. Here is an example of how to leverage ADKAR with the ICS Security Awareness short-course modules discussed in this poster:

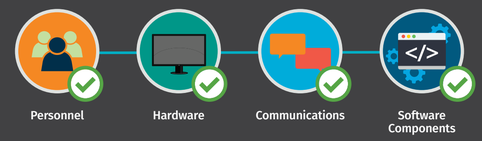
Awareness—Communicate the need for change by augmenting traditional IT security awareness with new ICS-specific training modules that contain knowledge checks and are aligned with safety. Highlight that ICS—its unique risks, threats, and consequences of ICS security incidents—is the business. Emphasize that everyone plays a role in ensuring safety and that ICS security is integral to supporting safety and engineering operations.

Desire—Foster a desire to support the change for control system roles and objectives. Highlight the importance of ICS security awareness for safety, reliability, and operational efficiency. Motivate stakeholders by showing how their involvement in ICS security enhances overall organizational resilience and safety.

Knowledge—Provide the knowledge to make the change to end user, engineering, and leadership roles, through ICS security specific modules and knowledge checks. Establish continuous monthly learning and tracking. Seek an engineering team champion who will help motivate and guide those needing extra support in understanding and retaining the necessary knowledge.

Ability—Employees need the ability to learn and retain new content through monthly security awareness campaigns. Enable success by providing ICS specific content in several forms: posters, information sheets, presentations, video models, and short tips as part of engineering safety moments.

Reinforcement—Reinforce the knowledge and the positive behavior through consistent reminders and ongoing monthly efforts with annually updated modules reflecting new ICS threats and aligned with safety protocols. The organizational change will be evident when the knowledge is applied and integrated into regular tasks and habits, embedding itself into the organizational culture aligned with safety.



CULTURE & ICS SECURITY BENEFITS

Dedicated ICS security awareness training modules are designed to enhance cybersecurity programs for engineering environments and align with safety first. Consider the following three primary strategic benefits:

1. Mature Cybersecurity Programs in ICS and Critical Infrastructure Sectors

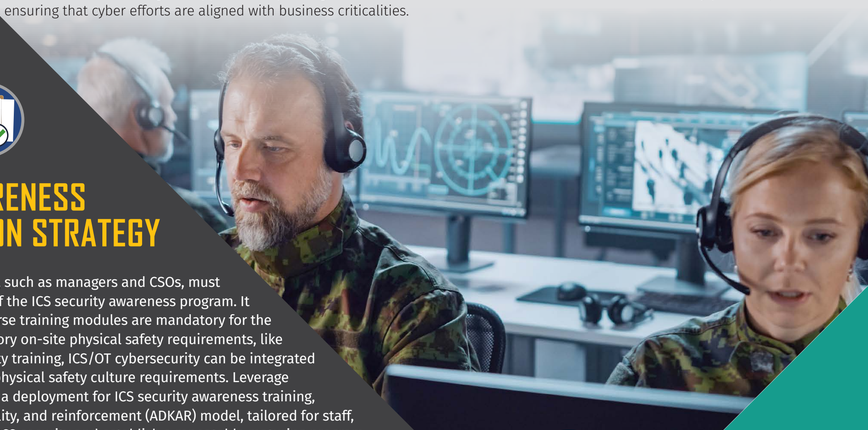
These modules are integral to thousands of organizations worldwide, where they are utilized by Chief Security Officers (CSOs) to either forge robust industrial security awareness programs from scratch or augment existing IT security awareness frameworks. The primary aim is to adeptly manage cybersecurity risks at industrial sites, thereby fortifying the overall security posture within critical infrastructure sectors.

2. Transform Cybersecurity Behaviors for Safer Industrial Operations

By adopting a practical and dynamic approach to risk management, these training modules not only evolve organizational culture but also focus on precise, targeted training. This strategy reinforces positive cybersecurity behaviors among engineers, end users, and leadership, ultimately leading to safer industrial facilities. The modules are designed to instill best practices and shift behaviors towards better cybersecurity hygiene.

3. Address Safety and Human Risks Associated with Cyber Events in Engineering

Leveraging industry-leading risk management methodologies, these training modules enable organizations to strategically focus their cybersecurity efforts where they have the most impact—the business operations within the control system environment. This targeted approach helps mitigate risks associated with human factors and enhances safety protocols, ensuring that cyber efforts are aligned with business criticalities.



SANS ICS SECURITY RESOURCES

ICS Engineer Technical Awareness Training

sans.org/security-awareness-training/products/specialized-training/ics-engineer

NERC CIP Security Awareness Training

sans.org/security-awareness-training/products/specialized-training/nerc-cip

Role-Based ICS Cybersecurity Training Modules

From plant managers and operations engineers to vice presidents of operations, everyone in the ICS hierarchy has an important role in protecting the infrastructure of major industries. Yet many of these individuals receive training better suited for the corporate environment, or worse, no security training at all.

Twenty-three brand-new ICS learning modules focus on the unique needs of ICS industries while equipping anyone who works within ICS environments, regardless of their expertise, with the information and tools necessary to protect and defend critical control systems.

ICS-specific Security Awareness Modules in this course have been targeted towards End User (E), ICS Practitioner (P), and Leadership (L) roles, as follows.

ICS END USERS (E)

Users will understand their crucial role in the overall mission of operational and engineering system defense. This includes their contribution to being part of the solution, regardless of their position or role, by examining a real-world example of a 2015 spear-phishing attack in Ukraine. Users will gain a comprehensive understanding of the interdependence and interconnectedness of systems and how they can be compromised, leading to significant impacts on service delivery through a range of real-world examples. Through an inspiring and positive story of employee awareness, users will gain insights into how they can contribute to identifying and addressing compromises. Users will learn about the unique risks posed by plugging in removable media, including how malware can be delivered and the implications of such actions on the system.

ICS PRACTITIONERS (P)

Practitioners will gain the knowledge to check configurations, assess the risk of mobile devices such as laptops, multimeters, and sensors in the system, and manage programs to reduce those risks. By adopting a cyber engineering perspective on system operations, practitioners will further enhance their defense capabilities against attacks and improve their responses through a real-world example. Practitioners will have an opportunity to explore a specific real-world incident and learn how to prepare for this attack surface. Practitioners will gain a deeper understanding of evaluating network architecture, operating through an attack, and best practices for operating in a disconnected model when perimeters become an attack pivot.

ICS LEADERSHIP (L)

Leaders will learn about key aspects of employing a supply chain risk management program, including addressing vendors, validating patches and files, managing breach notifications, and implementing remote access, with a particular focus on ICS. Comparative stories will illustrate the differences between IT and ICS/OT environments, incident response, and engineering recovery efforts.

Safety is #1 in critical infrastructure and control system environments. Safety is paramount and integrated throughout the training modules to align with the physical safety culture in ICS/OT facilities.

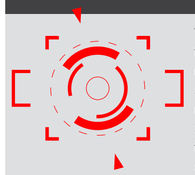
INTRODUCTION (E P L)

Industrial control systems are an essential part of every critical infrastructure sector. They have become increasingly interconnected, which exposes the systems to new cybersecurity risks. This introductory module kicks off the ICS Security Awareness series designed for engineers, control system operators, and other personnel responsible for maintaining safe operations and defending control systems and critical infrastructure against current and emerging cyber threats.

ICS OVERVIEW (E P L)

This module provides a high-level overview of what an ICS does, its typical components, the individual job roles and personnel who interact with it, and the common terms and technologies related to the ICS environment.

ICS ATTACK SCENARIO (E P)



This module dissects an example targeted cyber-attack against a specific utility and walks through the adversary actions step by step to show how a motivated cyber-attacker can gain access to an IT business network and then pivot into the control system environment. It is designed to help ICS personnel defend cyber assets and control systems as well as prepare to effectively identify and respond to an incident.

ICS UKRAINE ATTACK (E P)

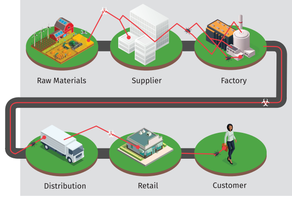
In 2015, adversaries breached three targeted electric utilities across different regions of Ukraine, causing widespread power outages in an unprecedented industrial cyber-attack. This module examines this real-world event from the perspective of the individuals working at the targeted utilities. This gives critical infrastructure operators insight into system defense and limiting the impact of an attacker within a targeted environment.

ICS INFORMATION ASSURANCE (P L)

Protecting information in the ICS environment requires detailed knowledge of the control processes, inter-device communications, risks to personnel and equipment, and device or process interdependence. This module reviews the use of cyber access controls and procedural controls to restrict access to system resources as well as the defense in depth network security approach.

ICS SUPPLY CHAIN SUMMARY (P L)

Supply chain attacks extend the ICS risk surface and can compromise system components and pose safety risks to asset owners and operators. This module covers software and hardware supply chain attacks and focuses on best practices and defense controls to prevent and/or mitigate supply chain attacks in critical infrastructure environments from software and hardware development to distribution.



ICS PHISHING (E P)

This module reviews phishing and spear phishing attacks, including a look at the 2015 Ukraine phishing attack that resulted in significant operational impact across the control system field environments. The focus is on understanding that cybersecurity is everyone's responsibility, regardless of their role in the organization, that any organization can be a target, and that people are the best defense against cyber-attacks within critical infrastructure organizations.

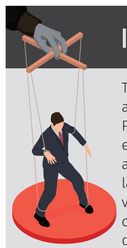
ICS REMOVABLE MEDIA (E P)

Various types of removable media devices are used for common operational and engineering maintenance tasks in ICS sectors, but they can also be targeted by adversaries to move onto a system. This module reviews the risks inherent to using removable media and the detection and mitigation controls ICS engineers can implement to reduce these risks.

ICS DRIVERS AND CONSTRAINTS (P)

This module reviews the four key drivers for securing an ICS environment—safety, reliability, security, and compliance. The module also studies common constraints of ICS environments, including the need for continuous monitoring, management, and control during operation, harsh industrial conditions and physical operating constraints, and personnel training and skills issues.

ICS OVERVIEW OF ATTACKS (P)



This module tackles different attack vectors adversaries may use within an ICS environment. Physical attacks, indirect physical attacks, social engineering, communications layer attacks, and attacks on the operating system and application layer are all outlined. Recognizing where vulnerabilities lie and implementing security controls that provide layered defenses and solid detection opportunities is crucial for ICS personnel.

ICS ATTACK SURFACES (P)

ICS environments have many potential attack surfaces where vulnerabilities can be targeted and exploited. This module covers the different ways an ICS can be at risk, including through people, network communications, control servers, and remote field devices. The "living off the land" attack approach is reviewed and steps to protect attack surfaces in an ICS environment are outlined.

ICS SERVER SECURITY (P)

Protecting control system servers is a critically important defense area. This module covers ICS-specific server security measures, including using a clearing house, securing remote access to the control system environment, using only dedicated and trusted transient cyber assets, designing environments to eliminate or reduce multiple component failures that could lead to larger system failures, and ensuring full restoration capabilities are tested and ready.

ICS NETWORK SECURITY (P)

Appropriate network security measures must be engineered into the ICS architecture to maintain the security, safety, and reliability objectives of the control environment. This module examines the three ICS network defense areas that must be addressed—the network architecture, network event detection, and incident response techniques.

ICS SYSTEM MAINTENANCE (P)

This module focuses on common ongoing control system maintenance tasks required for a secure and reliable ICS environment. These tasks include performing system backups, change management processes, patches and updates, monitoring, and logging.

ICS INCIDENT RESPONSE (P L)

This module covers ICS-specific incident response principles and actions. This starts with understanding the baseline ICS environment when it's running normally. From there, we can recognize when something is not normal and ensure that documented response procedures are in place and that personnel are properly trained. The module reviews the steps of an ICS-specific incident response plan—detection, containment, eradication, remediation, recovery, and restoration.

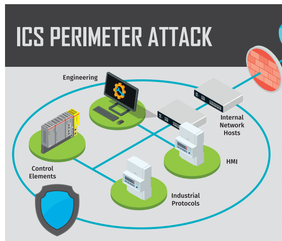
ICS TRANSIENT CYBER ASSETS (P)

Transient cyber assets such as laptops and engineering system calibration tools are commonly brought into the ICS environment by authorized personnel. If these assets are not secured, they introduce risk, increase the attack surface, and can be targeted by adversaries to gain system access. This module focuses on establishing a trust-and-verify approach for transient cyber assets prior to connecting to ICS devices, equipment, or networks.

ICS RANSOMWARE (P)

This module examines the interdependence and interconnectedness of systems, how they can be compromised, and the impacts on delivery. Two real-world incidents are studied—the 2017 Not Petya malware attack and the 2021 Colonial Pipeline ransomware attack. Preventive measures and security best practices to protect against ransomware attacks in ICS and critical infrastructure operations are reviewed.

ICS PERIMETER ATTACK (P)



ICS network perimeters protect internal critical devices and zones. This module focuses on establishing, maintaining, and defending a secure ICS network perimeter. The VPNFilter malware strain that targets network perimeter devices is also studied in this module.

ICS CYBER ENGINEERING OLDSMAR (E P L)

This module details lessons learned from a real-world event at a water treatment facility in Oldsmar, Florida in 2021. An intruder obtained unauthorized remote access to the control system. The module reviews the incident response activities, notification responsibilities, and actions taken by the employees to ensure the engineering process was not impacted as well as the protections that should be implemented.

ICS OPERATING THROUGH A RANSOMWARE ATTACK (P L)

This module takes a closer look at the 2021 ransomware attack against the Colonial Pipeline system and how it escalated to the point where the company had to shut down pipeline operations. The module emphasizes identifying and protecting systems that reside in between IT architectures and industrial or OT systems. Considerations for preparing to operate through an industrial attack and effective ransomware response actions are thoroughly covered.

ICS AWARENESS AND REPORTING (E P)

ICS and critical infrastructure personnel can be the best first line of defense against a malicious actor through their awareness and quick actions. This module discusses the 2021 real-world event at the Oldsmar, Florida water treatment facility from the lens of the operator's actions and communications immediately after becoming aware the system had been accessed. The module stresses the importance of knowing your organization's reporting process and notification obligations and your own job role's required actions in case of a security incident.

ICS CONCLUSION (E P L)

This module reviews the importance of security in industrial control systems and the need to build and maintain a defensible ICS environment and concludes the ICS Security Awareness series.

SANS
INDUSTRIAL CONTROL SYSTEMS SECURITY

ics.sans.org

ics-community.sans.org/signup
@SANSICS
linkedin.com/showcase/sans-ics
youtube.com/c/SANSICSsecurity

ICSSSA_ICS418_1124
Poster created by Dean Parsons—co-author of SANS ICS418 course.