A CSO'S GUIDE TO INDUSTRIAL CYBERSECURITY & SAFETY CULTURE

INTRODUCTION

This Industrial Control System (ICS) cybersecurity poster is for Chief Security Officers (CSOs), Chief Information Security Officers (CISOs), and others leading the charge in protecting critical infrastructure specifically in ICS and operational technology (OT) engineering environments. The leader's role in a mature ICS organization is to prioritize the security and safety of the engineering control system assets while providing executive decision-making and leadership in identifying, assessing, and managing risk.

In performing the responsibilities of a CSO or CISO, a major expected outcome is to bridge the gap between different departments and technology disciplines, manage unique engineering security challenges and risks, and deploy dedicated required resources, technologies, and unique practices to protect critical infrastructure engineering environments.

ICS IS THE BUSINESS

Proactive ICS security leaders prioritize safety of operations and assume already deployed preventative ICS security controls may fail at detecting brazen ICS attack techniques. Those responsible for ICS/OT security would do well to embrace the differences between IT and ICS/OT and prioritize the ICS, as ICS is the business.

Consider this example: two security incidents occur simultaneously; one on the IT business email system and another on the supervisory control and data acquisition (SCADA) system of a power grid to a region. Which incident should be prioritized to receive the needed resources to investigate, respond to, and defend against the attack? What pace and rigor will the organization give to the priority incident? Specifically, what drives the decision to manage these very different risks and very different consequences?

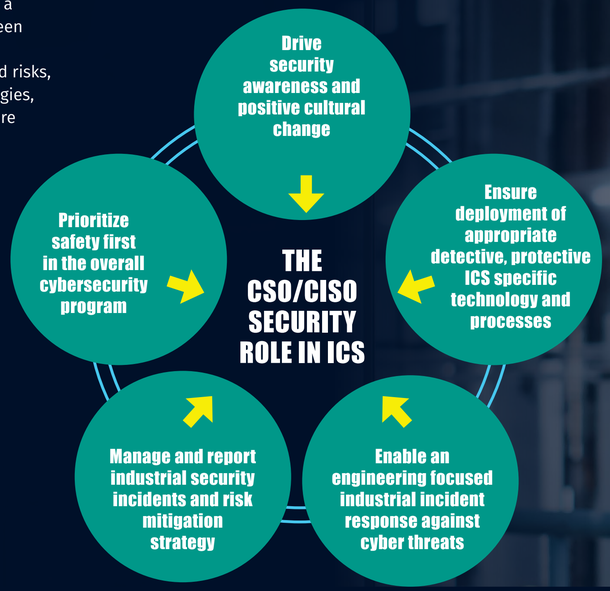
Safety could be at risk if IT and other traditional business support systems are prioritized over industrial engineering control systems. Likewise, safety is at risk if the responsible reporting structure for ICS security fails to fully embrace the differences between IT and ICS/OT.

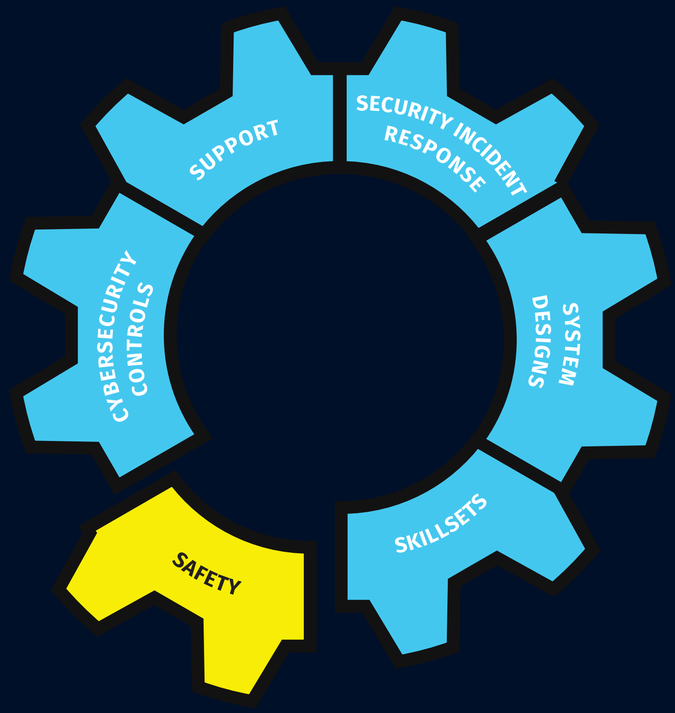
MATURE CSOs & CISOs EMBRACE IT & ICS DIFFERENCES

Industrial engineering control system assets are often inaccurately compared to traditional IT assets. IT and ICS systems have different missions, objectives, and impacts during an incident. They also have different devices, including but not limited to embedded operating systems and engineering devices speaking nontraditional industrial protocols. Adversaries targeting ICSs must use different attack tactics and techniques than in traditional IT cyber-attacks for access, execution, collection, and persistence to degrade safety, manipulate control, and damage physical engineering assets or property. Where traditional IT security focuses on digital data at rest or data in transit and the pillars of confidentiality, integrity, and availability, ICS/OT systems manage, monitor, and control real-time engineering systems for physical input values and control output for physical actions in the real world.

The six main areas where IT and OT/ICS differ are safety, security skillsets, system designs, support, cybersecurity controls, and cybersecurity incident response.

SANS
INDUSTRIAL CONTROL SYSTEMS SECURITY





HUMAN RISK DEFENSE LAYER IN ICS

> **The human element has been involved in approximately 80% of all breaches.**

This metric illustrates that security is not just a technology challenge but also a challenge in managing human risk. In managing an organization's culture.

As a CSO with industrial environments, you will need to ensure everyone plays their part in securing the critical infrastructure systems that power our world against cyber threats.

A first layer of the ICS defense in depth is policies, procedures, and awareness. Awareness means training and fostering a culture of ICS cybersecurity among ICS operators, engineers, and facility stakeholders. Security awareness is crucial to safeguarding all critical infrastructure in every ICS sector. It is foundational to a functional ICS defense in depth strategy.

As industrial control environments and engineering teams increasingly adopt new technology, threats through new vectors are taken advantage of by cybercriminals and nation state actors where the risk towards critical infrastructure also increases. ICS security awareness is no longer an option but a requirement. With targeted, easy-to-deploy ICS/OT-specific security awareness modules, facilities can deploy training, reduce human risk, and measure effectiveness and participation with quick knowledge checks. All of which is doable, measurable, and required for today's modern ICS/OT cybersecurity defense programs.

As the CSO, your organization needs ICS security awareness to help manage the human factor in control networks. ICS security awareness bridges the gaps and differences between IT and ICS while enabling the convergence of skillsets. A dedicated ICS security awareness program is part of every mature ICS facility security program.

CSO & CISO ROLES IN ICS CYBERSECURITY AND SAFETY

A CSO and other leaders responsible for ICS security should be highly dedicated to reducing physical safety impacts due to a cyber-attack. ICS leaders must effectively focus on tracking, measuring, reporting, and reducing related risks that could impact the safety and reliability of engineering system operations. ICS systems run electric power grids, water supply, oil and gas, transportation networks, manufacturing processes, and more. 70-80% of these environments could be running non-traditional operating systems, embedded engineering devices, and unique protocols. The importance of protecting and ensuring the safe operation of the critical infrastructure that supports our daily lives cannot be overstated. It requires a dedicated effort and teams with ICS specific skills, whereby only a portion of IT security skills apply, and in a nuanced way. It is critical as a CSO or CISO to ensure ICS cybersecurity staff have the appropriate skills for that job, where safety is their number one priority.

Safety training, drills, meetings, and stop-work safety protocols are commonplace in engineering environments. Impacts such as malfunctioning equipment or a cyber-attack on the control system network can have safety ramifications for facility workers and the environment, as well as the potential to disrupt or destroy physical engineering assets. As such, ICS organizations must have a strong safety culture. Even access to process control sites typically requires safety training and personal protective equipment (PPE), as well as safety training and certification, depending on the job role. These protocols are often required just to visit the facility. It is important to support and leverage the physical safety culture to create and maintain "Cyber Safety" initiatives. An organization with a mature safety culture understands safety is the first priority – even over security – and that security promotes and supports safety. For example, many organizations with mature Cyber Safety initiatives augment existing IT security awareness content with ICS/OT specific campaigns and modules and target many roles including leadership, end users, and engineering practitioners with this new ICS content.

A CSO'S GUIDE TO INDUSTRIAL CYBERSECURITY & SAFETY CULTURE

CHANGING CULTURE WITH ICS SECURITY AWARENESS

Dedicated ICS security awareness training modules are designed to:

1. Mature cybersecurity programs for ICS and critical infrastructure sectors.

Currently used by thousands of organizations around the globe, CSOs are leveraging these modules to build a new industrial security awareness program or expand their existing IT security awareness modules for the purposes of managing risk for their industrial sites.

2. Change cyber behaviors for safer industrial facilities.

A pragmatic approach to risk management, evolving culture, targeted training, and reinforcing positive impacts for engineering staff, end user, and leadership cyber behaviors.

3. Manage safety and human risk in engineering related to cyber events.

Industry leading risk-management methodology helps your entire organization focus cyber-efforts on the areas that matter most, the business, which is the control system environment.

CSOs, CISOs, and other ICS security leaders can manage human risk in engineering environments by considering the following elements as they prepare, assign, deliver, track, measure, and maintain ICS specific security awareness that is role-specific for their organization.

ICS SECURITY AWARENESS FOR LEADERSHIP

Leaders in ICS security must learn about key aspects of employing a supply chain risk management program, including addressing vendors, validating patches and files, managing breach notifications, and remote access, with a particular focus on ICS networks. Content should illustrate real-world case studies on the differences between IT and ICS/OT environments, incident response, and engineering recovery efforts.

ICS SECURITY AWARENESS FOR END USERS

Users must be educated to understand their role is crucial to the overall mission of operational and engineering system defense. This includes their contribution as part of the solution, regardless of their position or role. End users must be aware of the various types of attacks that are ultimately destined for the ICS environment. Users must gain a comprehensive understanding—through a range of real-world examples—of the interdependence, interconnectedness, and boundaries of systems and how they can be compromised and lead to significant impacts on engineering operations.

ICS SECURITY AWARENESS FOR PRACTITIONERS

Practitioners must be educated with the knowledge to check engineering device configurations, assess the risk of transient devices such as laptops, multimeters, and sensors in the system, and manage a program to reduce those risks. By adopting a cyber engineering-informed perspective on system operations, practitioners must also be educated—using real-world examples—to enhance their defense capabilities against IT and ICS attacks targeting control systems to improve their responses and engineering recovery capabilities.

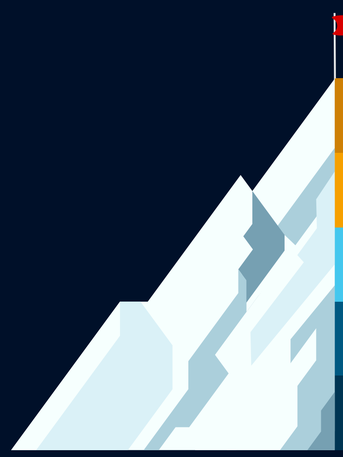
ICS SECURITY AWARENESS DEPLOYMENT

CSOs must measure the participation and effectiveness of the ICS security awareness program. Consider making participation in the ICS security awareness modules mandatory. Like mandatory on-site physical safety requirements—PPE, safety processes, and physical safety training. Include the built-in knowledge checks for tracking based on user and role. ICS risk leaders can leverage the ADKAR model tailored for process control engineering staff, operators, facility management, and facility administration staff to promote the importance of ICS security training as it relates to supporting safety of people.

ICS ENGINEER TECHNICAL AWARENESS TRAINING

SANS ICS role-based training modules empower individuals in critical infrastructure to effectively combat cyber threats. This innovative resource is a vital tool for organizations with ICS/OT environments. With ICS security incidents on the rise—nearly half of ICS networks have faced cyberattacks—ensure your organization is protected. Our top-tier security modules enable all ICS staff to adopt behaviors that prevent compromises.

SANS SECURITY AWARENESS



R – Reinforcement – The new ICS security awareness content will start making a positive change in the organization once it is part of the normal tasks and habits of an organization. The culture of the organization. The **reinforcement** will occur through regular reminders and continued monthly efforts, annually updated modules based on new threats to ICS, all aligned with safety.

A – Ability – People must have the **ability** to learn and retain the new material. Modules have knowledge checks. Effective security awareness campaigns are frequent. At least monthly. To promote employee's ability to successfully complete modules, throughout each month, provide ICS security awareness content (posters, information sheets, short tips) to prepare them before the modules are assigned with the knowledge checks.

K – Knowledge – Provide the **knowledge** of how to make a change – participating in, completing, and proving knowledge retention through knowledge checks on ICS security modules. All assigned roles can continue to learn monthly and apply their knowledge. The selected champion in the engineering team, as part of the CSOs ICS Security Awareness Cycle, can help motivate and guide those who may need extra support for the need for awareness, desire, and obtaining the knowledge in the modules.

D – Desire - Communicate the **desire** to support the change. Relate to control system roles and objectives as to why the change and focus on ICS security awareness is needed.

A – Awareness – Communicate the need for the change - augmenting IT security **awareness** with new ICS specific training and awareness modules. Communicate the unique risks, threats, and consequences when an ICS security incident is realized. Relay how everybody has a role to play in safety and that ICS security supports safety and engineering operations.

CSO TAKEAWAYS FOR ICS

Board-level owners and operators of critical infrastructure must understand what makes their organizations critical. It is their industrial control systems, i.e., ICS/OT, engineering, and operations. Leaders responsible for the protection and risk management of industrial control systems and critical infrastructure cybersecurity must:

1. Understand safety is #1.

In control system environments, safety is the top priority. Cybersecurity and other functions support safe and reliable operations. For example, tools like intrusion detection systems (IDSs) are preferred due to the side effects of false positives in intrusion prevention systems (IPSs) which render an unsafe condition that could hurt or kill people.

2. Embrace IT and ICS differences.

Understand and embrace the differences between IT and ICS by prioritizing the ICS business mission to secure and enable physics and engineering controls that monitor for and make physical changes in the real world that are safe for people and the environment.

3. Built the right team with the right skillsets.

IT, dedicated ICS cybersecurity training, and general engineering sector-specific understanding, always prioritizing safety first.

4. Mature the ICS security program.

Utilize the proper reporting and mitigations to manage the unique ICS risk by leveraging the safety culture through ICS specific security awareness.

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

SANS
INDUSTRIAL CONTROL SYSTEMS SECURITY

In a world that is seeing increasingly sophisticated and impactful industrial cyber threats, the below courses prepare OT security professionals to lead, defend, and protect industrial control systems at the foundational, management, tactical, and advanced skill sets. With SANS ICS Security, train to defend what makes, moves, and powers the world.

ICS CAREER PROGRESSION

		ICS Security Analyst	ICS Security Architect	ICS Security Incident Responder	ICS Security Leader	Process Control Engineering	ICS/OT Security Pen Tester
		Acquires and manages resources, supports, and performs key industrial security protection while adhering to safety and engineering goals	Ensures control system network security compliance and best practices for control networks	Executes specific industrial incident response for incidents that threaten or impact control system networks and assets, while maintaining the safety and reliability of operations	Builds and maintains business relationships with engineering staff and C-suite stakeholders by communicating and managing cyber-to-physical risks while reducing security risk to engineering operations and simultaneously prioritizing safety	Tests, programs, troubleshoots, and oversees changes of existing processes or implements new engineering processes through the deployment and operations of engineering systems and automation devices	Discovers system vulnerabilities and works with asset owners and operators to mitigate discoveries and prevent exploitation from adversaries
FOUNDATIONAL	ICS 310	**ICS Cybersecurity Foundations™** *Learn the cyber fundamentals to protecting ICS/OT environments*					
ESSENTIAL	ICS 410	**ICS/SCADA Security Essentials™** *Gain the essential skills to keep critical infrastructure safe from cyber threats*					
MANAGEMENT	ICS 418	**ICS Security Essentials for Leaders™** *Manage the people, processes, and technologies for OT cyber risk programs*					
TACTICAL	ICS 456	**Essentials for NERC Critical Infrastructure Protection™** *Maintain a defensible compliance program up to NERC CIP standards*					
	ICS 515	**ICS Visibility, Detection, and Response™** *Monitor threats, perform incident response and enhance network security*					
ADVANCED	ICS 612	**ICS Cybersecurity In-Depth™** *Identify threats in a real-world ICS environment to protect against adversary attacks*					
	ICS 613	**ICS/OT Penetration Testing & Assessments™** *Perform safe, hands-on ICS/OT penetration testing and assessments to identify vulnerabilities and improve operational resilience*					

Where multiple courses are shown for a given role, determination of the best course to take would be based on the number of years of experience and sector of work.