Industrial Control Systems Cybersecurity Assessment Tool

User Guide

The purpose of this guide is to provide users additional context and information on the Industrial Control Systems Cybersecurity Assessment Tool. The tool promotes awareness of cybersecurity risk areas associated with Industrial Control Systems (ICS) in industrial facilities. It includes 20 simple questions to characterize ICS and plant/facility operations and produces a preliminary assessment of risk (high, medium, or low). It also generates a customized list of action items to help improve preparedness for a cybersecurity event. This User Guide provides additional context for the questions included in the tool, clarifies their intent, and explains their relevance with respect to cybersecurity.

Section I includes additional information on the questions included in the assessment tool, including explanation of risk and background. Section II defines key terms included throughout the User Guide.

Section I: Background & Risk Explanation

People

1. Does your plant or facility provide basic cybersecurity awareness training to all employees?
Employee activities can pose risk to internal systems within a plant. Requiring employees to take regular cybersecurity trainings can help avoid accidental contamination of plant IT and control systems. To prevent unintentional damage, trainings should cover such material as:

- Password and privacy protection
- Phishing-attempt recognition
- Proper conduct with hardware (e.g., locking computers, reporting lost devices, updating anti-malware software, etc.)
- Plant boundary/physical security (e.g., sign-in and escorted access in facilities for vendors/guests)

Purposeful damage through employee conduct (e.g., an employee operating a machine outside normal operating bounds) is hard to mitigate through behavior change and is more effectively addressed through hardware controls like the closing of open USB ports, the installation of internal firewalls, and the imposition of alarms and standard operating parameters in machinery.

2. Are staff assigned and trained to take appropriate measures during a cybersecurity incident?
Responding to, and recovering from, cybersecurity threats/incursions in a timely way will mitigate much of the damage and cost associated with a cybersecurity attack. Downtime and capital repair/replacement costs typically represent the largest expenditures in a cybersecurity event.

As part of a cybersecurity incident response plan, an organization should identify and assign critical roles to ensure that the team is properly equipped for an incident. Some roles may be assigned to employees, and other roles may be assigned to outside parties, such as ICS vendors, manufacturers, and/or specialists with a dedicated focus on cybersecurity. To view additional guidance on organizing a team and a list of suggested staffing roles, download the U.S. Department of Homeland Security's *Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability*.

Specialized training should be delivered to staff with responsibility for control system operations. Knowing how to safely and promptly shut down machinery as well as evaluate IT assets for changes in operation or damage are the best avenues for cost mitigation following a cyber incident.

3. Do your industrial control system (ICS) vendors provide remote support?

ICS vendors typically help manufacturers set up and manage the operation of an industrial control system. Vendors can act as resources to support industrial control systems, and, when a cybersecurity (or other) event occurs, a vendor may be able to help mitigate the impact as they are well-positioned to respond to cyberattacks and rebuild, program, and clean the ICS after a breach.

This question is intended to assess in what capacity a vendor provides technical services and how specifically they support the manufacturer (e.g., vendors coming on site or using remote access). Vendors can assist with modifications to industrial processes, but they can introduce vulnerabilities to a facility if they are not properly trained (see question 5 below for more information on cybersecurity training). While allowing vendors remote access to internal systems may be valuable from an operations perspective, it introduces additional security risks. Remote access can provide an easy entry point for cyberattacks.

4. What level of on-site physical security does your facility or plant enforce upon vendors?

Vendor physical security is important, because vendors represent a potential weakness in the perimeter of your facility. Physical security involves securing a facility's network and hardware from external organizations. Components of increasing physical security for vendors would include restricting access to vulnerable facility locations, requiring escorts when a vendor is in a facility, and implementing surveillance systems. When making service visits, vendors present a potential risk of accidental virus transmission (e.g., a vendor plugging in an external hard drive that can have hidden malware).

5. Do third party vendors have proper cybersecurity training?

Vendors can pose a significant risk to internal systems within a facility because they routinely cross plant boundaries. Ensuring that an IT system remains protected in the presence of frequent vendor interactions requires regular inspection of vendor equipment and controlling access to facilities and computer systems. Through training, vendors can be better versed in proper cybersecurity conduct and avoid simple mistakes such as using personal external media devices at work or opening suspicious emails.

Proper cybersecurity training entails coaching by a knowledgeable IT professional and can cover a variety of topics, including response to cybersecurity threats in ICS environments, broad threat awareness and prevention, and ICS network traffic analysis. It may not be necessary for manufacturers to receive in-depth training with respect to all these topics, but some level of understanding can help. There are many certifications that an IT professional may obtain to demonstrate proper cybersecurity training.

6. Do vendors utilize their own equipment, hardware or software during site visits?

Hardware and software have the potential to carry unidentified viruses, so understanding exactly what vendors bring on site is key to maintaining a secure perimeter around your facility and ICS.

Process

7. **Have you identified critical equipment in your plant or facility that would cause disruption to your operations if they were compromised?**

Identifying critical facility systems can help prioritize actions to protect equipment and ensure that in the event of an emergency shutdown due to an external event/failure or an internal system failure, vital equipment can be given extra attention to avoid full-scale mechanical failures. Major disruptions can include both full or partial plant shutdown or incidents requiring significant expenditure in response to either a suspected or known cybersecurity incident.

8. **Does a plan exist to identify and isolate impacted assets, or shut down equipment as necessary in the event of a cybersecurity incident?**

Being able to shut down critical facility systems quickly will help avoid most of the mechanical failures that can happen during a cybersecurity attack and will reduce the overall risk to the facility.

An emergency shutdown plan outlines the steps to turn off components of the manufacturing process and internet connectivity during an emergency event to limit the extent of the event's impact.

9. **Does your plant or facility have a cybersecurity incident response procedure?**

Developing a cybersecurity incident response procedure may start with a plant/facility establishing an inventory of critical equipment (question #7) and developing a plan to isolate and shut down those key assets (question #8). This procedure would likely be utilized during and after a shutdown to either ensure that no major issues resulted from the incident or identify the cause of issues.

These items may be part of a broader document. A cyber incident response procedure helps ensure that a team has the appropriate resources and recognizes critical actions necessary to respond to various incidents, including severe weather and cyberattacks, should they occur. Key elements of a cyber incident response procedure include:

- Overview, Goals, & Objectives
- Incident Description
- Incident Detection
- Incident Notification
- Incident Analysis
- Response Actions
- Communications
- Forensics

For more information on developing a response procedure, download the U.S. Department of Homeland Security's *Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability*.

10. Does a central repository containing equipment schematics, IT infrastructure drawings, and system network layouts exist within the facility?

By maintaining a central repository for IT information separate from the plant's IT system (i.e., on an isolated computer, on a mainframe, or in a physical file), a team can ensure that critical information remains accessible when the IT system may be shut down during a cyberattack or system outage.

11. Is cybersecurity considered when purchasing supplies or equipment, and is it defined in your contractual obligations with vendors?

When selecting new equipment or software for the plant or facility, security should be a consideration. Device connectivity, software configurations, regularity of software updates, and vendor reputation are key areas for evaluation.

Incorporating cybersecurity obligations in your contractual documents can keep both parties up to date on cybersecurity concerns and will help ensure that cybersecurity is a component of technical scope and discussions.

12. Does plant/facility equipment get regularly or automatically scanned for cybersecurity issues (e.g., malware, etc.)?

Security scans identify viruses and malware that can interfere with normal equipment operation, send personal data to unauthorized parties, and/or grant access to private computer systems. Security scans can also identify software products that require updates or patches that were created in response to specific cybersecurity threats.

By performing scans regularly, a plant or facility can ensure the integrity of most systems and avoid major security risks. The automatic scheduling of security scans helps ensure that scans are not missed due to human error.

13. Is the use of external media by staff and vendors regulated within the plant/facility and scanned for cybersecurity issues?

Any physical access to a computer can be leveraged by an attacker. As such, any device that is connected to an IT network, including external media devices, must be properly managed. By developing and implementing a removable media policy that outlines approved memory devices and proper use, a facility can minimize the risk of exposure to external sources of malware and virus exploit.

USBs are the external media devices that are most likely familiar to a broad range of users in manufacturing facilities. Other external media devices, including external hard-drives and disk drives, pose similar risk to a facility.

Technology

14. Which of the following best describes the industrial controls in your plant or facility?

The types of controls and computers used in concert with an ICS can help determine the level of risk within a system. Antiquated, unpatched, or widely available operating systems (e.g., Windows) can represent a significant threat as cyberattacks are constantly evolving.

This question refers to the hardware elements of the ICS (the console or pneumatic/physical system) and its operation. Control system types:

- Operated using levers, pneumatic switches, and manual controls
- Manually operated machinery with minimal connectivity between different hardware elements
- Automated facility with multiple ICSs to control various stages of manufacturing
- Automated facility with a single ICS across all stages of manufacturing

In highly integrated or automated systems (automated facility with one or more ICS), the risk of mechanical failure due to a cybersecurity breach is much higher than in manually operated systems and those with minimal connectivity between different elements.

15. Are indicators or alerts set up on critical equipment to indicate unusual changes to operating parameters, multiple login attempts, or detect other anomalies in use?

Critical equipment includes high-value assets that are necessary to the organization's mission or provide an important security function. When regular operation of critical equipment is disrupted, there may be negative financial implications, due to missed production and/or equipment repairs.

When indicators or alerts are placed on digitally-operated machinery, plant or facility staff can be notified when the machinery operates outside typical bounds. When alarms are operating properly, they can indicate a cybersecurity (or other) issue, limiting damage to assets.

16. Does the plant or facility have any equipment that is programmable or reconfigurable by remote staff?

Reconfigurable machinery is not uncommon in manufacturing settings. This machinery can represent a threat if the ability to reprogram is not controlled in some way (either by user permissions or another IT protection).

Ideally, equipment installed by external entities (including ICSs) cannot be reconfigured without an identity verification process. This provides high risk protection, as it is harder for cyberattacks to compromise plant systems by modifying code that is protected from most modifications.

17. Does your industrial control system (ICS) allow remote access?

See the explanation for question 3 and 16 above. Risk applies to both employees as well as vendors.

18. Are there processes in your plant with operating parameters that are interdependent with other processes?

This question refers to equipment processing that automatically changes based on input data from elsewhere in the facility—generally downstream processes are responsive to the results of earlier, upstream processes. If data is compromised, this can allow viruses or bad actors to gain control of equipment. Processes that may be most at risk are those that are responsive to earlier processes in production via data transfer.

Mechanical failure risk is principally driven by machinery that acts in an automated way based on input data from upstream manufacturing processes. For example, in a facility where plywood is manufactured, the hot glue extruder may control the pressure at extrusion by examining input data about the viscosity of the specific glue type. If a bad actor were to compromise and alter that data, this could lead to mechanical problems in the extruder.

19. How are modifications to parameters or set-points made within your manufacturing process?

Modifications made to an ICS are typically made through a computer console or manual action(s).

Depending on the type of console, risk may be heightened or diminished.

- A PC running a standard operating system, like Microsoft Windows, poses the highest risk. The ubiquity of Windows has resulted in a greater influx of attacks targeting the Windows operating system.
- A PC running a specialized control system software poses a lesser threat. There are fewer cyberattacks designed to target specialized software programs, though they do exist.
- Manual operating switches and values pose minimal risk, as control of the system cannot be taken by a remote party.

20. Do the computers that run your industrial control system (ICS) allow employees or vendors to import files from external media?

When electronic files can be imported to ICS-associated computers from an external media device, such as an USB drive or disk drive, the computers are at risk for both accidental contamination and purposeful damage from malware (see question 1 above for more detail).

Section II: Definition of Key Terms

Accidental Contamination: inadvertent exposure to malware or other cyberattack due to employee or vendor action, such as improper password or hardware protection, opening of phishing attempt emails, or facility security.

Assets (IT, high value): information or system that holds or transmits high-value information pertaining to the organization. In particular, information or systems that are necessary to the organization's mission or provide a critical security function.

Central Repository: a central place where system layouts, diagrams, and data are located.

Critical Facility Systems: the systems without which the plant could not function for an extended period. These systems may be expensive or difficult to replace due to complexity or availability of vendors/suppliers. Examples include machinery necessary for plant production and the facility operating network that allows for communication between employees and devices. These critical systems should be the focus of cybersecurity protection as they are the most likely to cause large disruptions in plant operations.

Cyberattack: attack or destruction from individuals, groups, organizations, or states seeking to exploit dependence on cyber resources, either for financial gain or malice.

Cybersecurity Risk: any source of potential attack or destruction to an organization's data and assets. Threats include all possible causes of any type of security breach, including deliberate actions from outside parties and accidental activity from authorized users.

Data Transfer: transmission of data over a network to enable communication between different systems/equipment.

Downstream Processes: production stages that are later in the process (closer to end-product).

External Event/Failure: failure of critical infrastructure on which the organization depends; threat comes from outside the control of the organization (electric grid, internet, etc.).

External Media: removable device that stores information electronically, including both USB-drives (e.g., "USBs" or "flash drives") and external hard-drives, as well as disk drives.

Hardware: physical components of the organization's IT and industrial control systems. For a computer, hardware components include the monitor, hard drive, and CPU.

Industrial Control Systems (ICS): general term that encompasses several types of control systems and instruments used for industrial process control.

Internal System Failure: failure of equipment, environmental controls, or software due to aging, source depletion, or other circumstances that exceed expected operating parameters**.**

Malware: software that is intended to damage or disable computers and computer systems.

Operating System: software that manages a computer's hardware resources, including input devices (e.g., keyboard and mouse), output devices (e.g., monitors, printers, scanners), network

devices (e.g., modems, routers, and network connections), and storage devices and allows a user to run other applications.

Physical Security: efforts to reduce cybersecurity risk via increased facility security, including sign-in requirements and escorted assess for vendors and guests.

Purposeful Damage: willful exposure to malware or other cyberattack due to employee or vendor actions.

Remote Access: the ability to access a computer or network from a remote location. This encompasses both employees working from home locations, as well as other corporate locations.

Secure Perimeter: a network perimeter with all boundaries between the locally-managed side of a network and the public side properly secured from intrusion and other vulnerabilities.

Software: the programs and other operating information used by a computer.

Upstream Processes: production stages that are earlier in the process (further from end-product).

Vendors (ICS): individuals or companies that help manufacturers set-up and manage the operation of an industrial control system, including software and equipment companies and service providers.