Where to Start in Cyber Security

A guide for how to plan, implement and maintain an effective cyber security program for energy industries.

Contents
01 Today’s threat and vulnerability landscape
03 Where to start
04 Focusing on the fundamentals
05 If not now, when?
Introduction

The industrial world is becoming more digitally connected, making operations smarter and more productive. But with that connectivity comes vulnerability. Cyber security is now a reality of business in our connected world. Industrial Control Systems are a frequent target and need to be protected.

In our world of on-demand services and smart phone apps that provide quick and easy solutions, our tendency is to think that the latest and greatest technology will be the silver bullet to solve our needs. But, when it comes to cyber security in the world of Industrial Automation and Control Systems (IACS), there is no silver bullet—no single app that can make cyber security threats go away.

The answer is in the fundamentals. Applying basic cyber security practices can greatly reduce an organization’s risk of plant outages and operational disruptions due to cyber security threats and vulnerabilities. The goal of this paper is to focus on the fundamentals: what today’s cyber security landscape looks like and what basic steps an organization can use to start to create a more secure environment for their IACS.

Today’s threat and vulnerability landscape

In 2016, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) reported 290 attacks in the US against control systems, with the systems governing energy production and distribution being the second biggest sector hit. This issue is common across many countries.

Whether cyber incidents are caused by outside hackers or nation states, or are a result of careless or accidental actions by authorized users, the risk for interruption to operations is the same.

By examining three environmental causes related to these occurrences, we can start to understand the areas of opportunities to improve security posture.

1. Technology lifecycle. Most plants constructed prior to 1990 had very few integrated systems that use standard routable protocols common to the internet. Back then, systems were relatively isolated and used proprietary, non-routable, and even non-electrical mechanisms and protocols for control and communication. Many of these plants are still using older control systems, with very few going through extensive upgrade efforts.

2. Target-rich environment. Plants built after 1995 have more electronic, intelligent devices that use standardized routable protocols. Many of these plants are built with TCP/UDP/IP based integrated control, protection, and safety systems. An example of a large OT environment is a medium to large gas processing facility with up to 1,000 TCP/UDP/IP enabled devices from 100 different vendors. Compare this to a large data center that can have more than 50,000 TCP/IP enabled devices spread across fewer than 15 vendors. A relatively small technical makeup from a limited number of vendors in a traditional IT environment makes it easy for staff to manage and keep all the systems patched, monitored, and up-to-date. And, if mistakes are made in IT environments that require a system rebuild or reboot, the consequences of this unplanned outage will most likely not be as severe as in the IACS environment.

Terms to Know

**Attack Surface** – An information system’s characteristics that permit an adversary to probe, attack, or maintain presence in the information system.

**Operational Technology (OT)** – The hardware and software that is used to acquire, store, monitor, and control plant systems and related data that are used for process control, management, and safety.

**Process Control Network (PCN)** – The computer network that hosts the systems used for process control, monitoring, and safety functions. Unlike traditional IT networks, PCNs host systems that have cyber-to-physical interfaces.

**Security Posture** – The overall cybersecurity strength of an organization. This includes the relative security of IT applications, as well as hardware and software, and how they are managed through policies, procedures or controls.

**Supervisory Control and Data Acquisition (SCADA)** – A category of software application programs for process control that involves the gathering of data in real time from remote locations in order to control equipment and conditions.

**Threat** – Something that could cause harm to a system or organization.

**Threat agent** – A person who performs a cyber attack or causes a cyber incident, often for malicious reasons, kudos or personal gain.

**Vulnerability** – A flaw or weakness that can be used to attack a system or organization.
The criticality and diversity in the software and hardware technical makeup of an OT environment make system maintenance and patch management quite challenging. Complex, critical asset technology, diverse vendor footprint, and staff with little to no cyber security skills make it easier for threat agents to use their knowledge and expertise to take advantage of the operation. These factors make IACS attractive to exploit and monetize.

Different from those built before 1995, the devices in the more modern plants are connected. However, they were put into operation before current cyber security technical controls and processes were developed, or even needed. Even fewer will be under the umbrella of a complete cyber security management program that addresses all phases of the plant lifecycle. Furthermore, the multi-vendor footprint that makes up an IACS means these systems are more difficult to patch and monitor.

Large operators may have begun the work of defining cyber security requirements, but, due to constrained resources, the application of these requirements may be inconsistent at the plant level compared to the headquarters directive. For some organizations, the risk of an incident is not quantified well enough to justify the cost and perceived disruption of plant operations that is required to implement cyber security controls.

3. **Threat agents.** One of the many differences between OT and IT environments is physical access control. For OT, there are a variety of people who have access to control rooms, equipment rooms, equipment buildings, and staging areas. Each of these areas contains devices from many different vendors and have multiple ingress points into the process control network. While multiple people may have access to an IT community, IT is typically not as vast as its OT counterpart. In addition, the level of accountability and cyber security awareness of the people coming and going will be inconsistent.

In an OT environment, contractors and employees converge together to operate and maintain numerous assets and systems. The basic screening and safety training given prior to gaining access may not be enough to ensure responsible security behavior. It is common to see unscanned laptops and removable media used to troubleshoot and maintain the equipment within these rooms. In addition, low-cost, 3G and 4G mobile routers are readily available to enable access for short-term remote support.

To date, the most infamous malware events within the OT community were most likely nation-state initiated. Historically, the motivation for these attacks is strategic or retaliatory; however, new threat agents targeting OT and critical infrastructure today may now include profit-driven, cyber-criminal organizations. In the past, knowledge of OT environments was mostly limited to people working in that field. Today, these criminal organizations are looking for new markets to exploit. They are well organized and have developed extremely high levels of competency with their many years’ experience exploiting other business sectors for profit.

OT cyber security and vulnerability exploitation has gone mainstream. News articles are released daily. Security conferences are focused on the topic. Governments around the world are aware of the risks and are working to regulate the industry. But with the efforts to combat cyber threats, the hacker community continues to grow and adapt. As monetization opportunities in...
traditional environments such as financial services, retail, and commercial operations are shrinking, threat actors are focused on the new target of OT.

OT vendors and integrators need to adopt best practices that focus on security throughout design, development and delivery. While these practices may not eliminate future vulnerabilities, they can help to better prepare the organization for cyber threats. In addition, following standards such as IEC 62443-2-4 can help operators set expectations for vendors and integrators.

The combination of motivated cyber-criminal organizations, easy-to-access knowledge, off-the-shelf technology, and numerous vulnerability databases have provided the ingredients helpful for threat actors to cause disruption and profit through the exploitation of businesses that rely on digitized systems for plant safety, control, management, and operation.

Where to start

Determining where to start developing a cyber security management or remediation program can seem like an intimidating task. There are several low-cost and free activities that can and should be done before any substantial amount of money is spent. Many of these items can be done in parallel.

1. Review existing standards and documentation.
   a. Start from the inside out. Check to see if there is already a set of guidelines or policies in place at your organization. If you are involved in any joint ventures, see if there is anything they can share. Talk to your IT team.
   b. Check your local government services. Many countries are running Cyber/Computer Emergency Response Teams. Many of these teams have created cyber security standards and are willing to share them.
   c. Review the free standards. The NIST 800 series are free to download. NIST 800-82 is especially relevant for the scope of industrial control systems. NIST has also published the Framework for Cyber-Physical Systems. Even though it was developed for North America Power Producers, NERC CIP is useful and can be applied in other regions and industries.
   d. Review the paid standards. IEC 62443, which has superseded ISA 99, is another useful set of standards. This is the first international standard released that covers operators, vendors and integrators. The cost to purchase is low, and the content is worth the price as it addresses all phases of the cyber security management life cycle. The ISO 27000 series is informational, but it does not include a lot of information specific to OT environments.

2. Review systems architectures and IP address schemas.
   a. Most companies have these. Find yours, and don’t assume they are accurate.

3. Conduct a baseline inventory.
   a. Conduct an inventory of all the TCP/UDP/IP enabled and serial devices within your operations. This step is critical, so make sure you are not using information from past diagrams. Conduct a thorough and detailed walk down of your facilities.
      i. For each system discovered, document the system vendor; IP information; model; serial number; location; purpose; and process. Try to figure out what it talks to and how it’s connected.
      ii. Look for RJ-45 connected systems, fiber optic connections, and various serial connections. For less-known systems, be on the lookout for DB/DE-9 and USB to serial adapters. Within the OT landscape it is common to convert media types.
      iii. Some of these systems can be very old, may be a single point of failure, and can be fragile—so handle gently.
      iv. Finally, if the plant is in service, don’t use any active scanning tools on your network to help find or create the inventory of your assets. This could very easily lead to systems locking up, becoming unresponsive, and shutting down the plant process.

4. Start the gap analysis.
   a. Compare what is in the document repository and what was discovered during the site(s) walk down. Note any discrepancies.

5. Categorize your assets.
   a. Now that you know what is out there and have an inventory, use the guidance of IEC 62443-1-1 to classify the items found.

6. Build an industry network and expand your knowledge.
   a. Consider joining a group such as WIB or the Industrial Control Systems Joint Working Group (ICSJWG).
   b. Attend free training such as ICS Cybersecurity 301.
   c. Attend a free user’s conference such as ICSJWG.
By completing the items above, you will gain a strong knowledge of your assets and familiarization with cyber security topics. If you choose to hire an outside company to conduct the inventory, gap analysis and other activities, make sure to understand their plan for your program by comparing it to the steps above.

Site Security Assessment

One of the key components to help secure funding and gain leadership support for a cyber security management program is tangible data that shows the current cyber security health of your site. This is best accomplished by conducting a site security assessment. The output of this assessment, along with the knowledge and experience gained from the steps listed above will provide the business justification needed to implement some measure of cyber security technical controls or perhaps even a complete cyber security management program. Data should focus on the possible risk of interruptions to operations driven by a cyber security incident. The output of the report along with a quick risk assessment can be used to quantify how cyber incidents could impact human safety, environmental safety, asset health, company profitability and reputation. To get the most benefit from the site security assessment, items 2 and 3 mentioned above in the Where to Start section should be complete.

The site security assessment should produce a list of specific and actionable observations and recommendations. This information helps provide additional justification for cyber security investment.

IT/OT Convergence

While IT teams, along with their associated processes and technologies, can be placed into OT environments, some fundamental differences exist. Due to the high volume of vendors involved in OT environments as well as the criticality of the systems, it is not reasonable to expect the same bulk management processes to work in OT that are used in IT. Patch management is a good example of how using IT processes may cause issues in an OT environment. The deployment of the patches must be properly staged and planned for so as not to create interruption. Patches should always be approved and qualified by the application vendor, not the OS vendor. Some systems may not even be patchable thus requiring other forms of protection.

A successful OT cyber security management program brings resources from both enterprise IT cyber security and OT spaces together to share knowledge and responsibility.

Focusing on the fundamentals

Two resources worth reviewing to understand the fundamentals of technical controls for cyber security are: “Seven Strategies to Effectively Defend Industrial Control Systems” published by the US Department of Homeland Security’s ICS-CERT organization and “CIS Controls for Effective Cyber Defense,” published by CIS – Center for Internet Security.

The Seven Strategies report—based on actual incidents that were reported to ICS-CERT in 2015—is free to download, and is useful for the OT community with recommendations driven by real-world incidents.

Although CIS is not an organization that specializes in OT and its report is not based on data from OT real-world incidents, the controls suggested by CIS are worth reviewing.

In both cases, there is a common theme of keeping environments safe by focusing on the basics. Per the Seven Strategies document, 67% of reported incidents could have been avoided by implementing two technical controls: application whitelisting (38%) and patch management (29%).

Application Whitelisting

Application whitelisting runs on Human Machine Interfaces (HMIs) and helps to secure the endpoints from unwanted applications by designating only the specific applications allowed to run on the ICS network. The difference between traditional anti-virus blacklisting and application whitelisting is that blacklisting only protects from known malware while allowing all others through. Whitelisting allows only approved applications, which means those threats that are bad but have not yet been identified by traditional anti-virus blacklisting are still prevented from reaching the control system.

Application whitelisting is an important tool as we see an increase in smartphone users and applications that tend to also create an increase in malware risks. In addition, Zero-day threats and Distributed Denial of Service (DDoS) attacks are examples where blacklisting is not effective. They are initially unknown, and therefore, not on the blacklist. These targeted, covert attacks are being deployed more frequently and use techniques specifically designed to evade blacklisting.
Patch Management

Patching your systems, or updating software and signatures, is one of the best things you can do to protect your assets and assure the operating systems and programs on your endpoints have the latest protection. Patching of application and system software is vital to improving and maintaining a high security posture. Loss of process view and control can occur when HMIs are compromised, but maintaining a regular rhythm for updating the operating systems as well as the applications, can help prevent access through your endpoints.

Reduce Your Attack Surface Area

A third step to take is to reduce your attack surface area, which per the Seven Strategies could mitigate 17% of incidents. Per the report, reducing the attack surface area consists of easy-to-implement items such as:

- Locking down unused ports
- Disabling unused services
- Using uni-directional optical separation technologies for communication between the OT network and non-OT networks whenever possible

The large number of cyber security incidents around the world, whether external or internal, uncover weaknesses or failures in cyber security systems that can often be avoided. When attack surfaces are uniformly and consistently addressed, technical controls can be implemented or corrected to provide suitable protection and improve security posture.

Think of this in relation to the things we do to protect ourselves in our daily life: properly managing passwords for our accounts; maintaining anti-virus software on our personal computers; and being careful not to download attachments from unknown email recipients. These efforts are all a part of reducing your attack surface by limiting the number of ways that you are vulnerable to a cyber threat by using multiple means to protect yourself. These practices are just as important in the industrial space as they are in our personal space.

Efforts in the three areas mentioned above could have helped prevent 84% of the reported incidents in 2015.

If not now, when?

243 days. That’s the average number of days a system is compromised before the intrusion is discovered. Whether your organization is willing to fund a full blown cyber security management program, or take small steps against vulnerabilities, it is highly advisable to begin protecting critical assets as quickly as possible. It is not necessary to wait for the program to be fully defined, approved, and tested before you take basic action.

An established and mature cyber security management program consists of a framework of policies, guidelines, and procedures that cover all aspects of plant and systems lifecycle. The definition of such a framework can take many months to accomplish. The implementation, operation, measurement, and monitoring activities take even longer. In total, for large organizations, it can take years to go from plan inception to implementation.

The idea that a perfect program, a silver bullet solution, or a quick fix technology will solve your cyber security challenges should not be a part of your plan. Changes will need to be made. Re-work will happen. Cyber criminals will continue to learn and adapt.

The recommendation is to do things in parallel. As the cyber security management program is defined, begin to implement technical controls to protect critical assets. Apply the knowledge specific to your organization and industry along with data-driven advice from “The Seven Strategies to Effectively Defend Control Systems.”
References

3. NERC CIP Regulation - http://www.nerc.com/pa/CI/Pages/Transition-Program.aspx
4. IEC 62443 International Standard - https://webstore.iec.ch/searchform&q=IEC%2062443