Cybersecurity: You Cannot Secure What You Cannot See

Follow this guidance to understand today's cybersecurity risk landscape and take the necessary steps to create a sound industrial control system cybersecurity program, including the development of a comprehensive, in-depth cyber-asset inventory

David Zahn
PAS, Inc.

In industrial facilities, cyber incidents typically result from three basic scenarios: a malicious attack from an outside individual or group; a cyber incident that results from an engineer making a mistake that alters a control process or diminishes safe operations; or the work of a disgruntled employee or ex-employee. No matter which of these scenarios you believe is real or presents the most risk, companies must take steps to protect their industrial control systems (ICS) from cyber incidents. What should companies do and how far should they go to ensure that risk is managed to a sufficient level? This article addresses the fundamental elements that an ICS cybersecurity program must contain, and shares guidance on how to develop an in-depth cyber asset inventory.

FIGURE 1. Cybersecurity risks can arise from several scenarios — malicious attack, human errors and the intentional actions of disgruntled current or former employees

Cyber incidents

A malicious attack from an outside individual or group. Although such attacks have affected physical operations in a number of well-publicized cases, most outsider attacks to date have focused on proliferation and reconnaissance (get in, spread, gather information, and report back) as their primary objectives. The passive nature of these attacks has lulled many into believing there is more hype than reality in the likelihood of a malicious attack. Most cybersecurity experts would agree that attacks of this type to date are merely a prelude to attacks that will take more directed action in the future. The attack on a power plant in the Ukraine in December 2015 in which hundreds of thousands of people lost power in the dead of winter is a testament to what is to come.

A cyber incident resulting from human error. These mistakes can go undetected until it is too late. Most engineers who have worked in chemical process industries (CPI) facilities long enough can share stories of when such incidences have occurred.

The work of a disgruntled employee or ex-employee. With the spate of layoffs during the last several years — particularly in the oil-and-gas sector — the potential for an insider threat is a rising concern for chief information security officers. Georgia-Pacific recently incurred the wrath of a fired employee who, soon after being laid off, accessed and altered control systems from his home. The company required a significant amount of time to recover from the damage he had inflicted. That employee was successfully prosecuted.

Know your cyber assets

In the race for better ICS cybersecurity, CPI companies all face the same challenge — knowing what cyber assets they have in the plant. Operators and managers tend to have good insight into the non-proprietary assets, such as workstations and routers, but they often lack sufficient visibility into the proprietary assets that run critical processes and keep plants safe. This lack of visibility introduces a level of risk that negatively impacts cybersecurity, safety and compliance efforts.

To what extent does this lack of visibility exist? In one real-world example, an inventory at a plant site showed that 20% of the cyber assets were traditional information technology (IT) systems that standard protocols — for example, Windows Management Instrumentation (WMI) and Simple Network Management Protocol (SNMP) — could interrogate for detailed configuration information. These systems include Microsoft Windows workstations, servers, routers and switches that sit in front of the proprietary control systems. An inventory of these is important to have, but it only paints a

partial picture of what is happening within the overall control network.

In our example, the remaining 80% of cyber assets came from the proprietary industrial control systems, such as distributed control systems (DCS), programmable logic controllers (PLC), or safety instrumented systems (SIS). Unlike a workstation, ICS systems have no standard protocols to pull detailed configuration information (such as I/O cards, firmware, software installed, and control strategies).

There is also no option to put an agent on such systems to push data out, as doing so invalidates vendor support. These systems give hackers the greatest opportunity to wreak havoc in a plant, and they also create opportunities for well-intentioned engineers to make mistakes that adversely affect operations.

FIGURE 2. Knowing, in detail, the full extent of the facility's (and the company's) cyber assets is a critical step for developing a plan to both prevent and respond effectively to potential cybersecurity threats

Create a cyber asset inventory

Efforts to collect an inventory of cyber assets within a control network typically take three forms — manual, vendor-supplied, and IT-only. The following discussion examines the positives and negatives of each approach.

Manual inventory. Manual gathering of inventory data is the most prevalent approach used today. Companies will send engineers into plants to perform a physical inventory, and they will gather a limited set of common data points, related to such information as manufacturer, model and version. The data are consolidated in a spreadsheet and used organizationally.

This approach is convenient, but is not economical, because engineers walking a plant are expensive resources and having them carry out inventory duty has high opportunity costs. Similarly, the manual gathering of inventory data is inherently prone to errors due to the human element, and this approach will typically yield an incomplete assessment, potentially missing swaths of important information, including control logic and shutdown interlocks. Such a data inventory can also quickly become outdated over time. Finally, there are few options for automation using a simple spreadsheet, as such a tool does not enable security policy monitoring and management-of-change processes.

Vendor-supplied solutions. Control system vendors often provide a managed service offering that essentially throws additional outside help at manual inventory efforts. All of the problems with a manual inventory still exist, but internal resources noted previously are freed to do other high-value duties. Many vendors will also offer tools to manage cyber asset inventories, but these tools rarely extend beyond their own control systems. Companies that adopt such tools run the risk of creating solution silos that ultimately add complexity to a cybersecurity

According to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), effective physical and environmental protection requires "a detailed inventory of all hardware and software components utilized in support of operations, including detailed information pertaining to device/model type, serial number and firmware version" [1].

environment. Complexity is counterproductive to building an effective ICS cybersecurity program.

IT-only solutions. There are many solutions available that can discover non-proprietary systems and provide detailed configuration information, as well as advanced analytics. Such products are quite good at these tasks and given the number of solution providers with such capabilities, this has become a commodity offering. CPI companies must have non-proprietary information as part of their cybersecurity program.

However, they must also recognize that the resulting data come from only about 20% of the cyber assets in a process control network. Ultimately, IT-only solution architectures cannot scale to include the much more complex, proprietary systems that comprise the remaining 80% of cyber assets in a plant.

Exploring 'Inventory in Depth'

A best practice solution must overcome the limitations of today's approaches to inventory. It must gather inventory data for both non-proprietary and proprietary cyber assets, it must contain deep configuration information, and it must break down data silos so that the wide variety of manufacturer control systems are made visible.

Next, we explore the elements for developing a best practice, comprehensive cyber asset inventory. We'll refer to the end product as Inventory in Depth.

One database to rule them all. The first element of an Inventory in Depth approach is to have both non-proprietary (IT) and proprietary operational technology (OT) data in a single repository. The ability to carry out automated vulnerability assessments, security policy enforcement, unauthorized change investigations, patch management processes, analytics and more is only as good as the breadth and depth of the inventory such efforts utilize. Gathering OT and IT assets into a single database ensures breadth; ensuring depth requires having all configuration data, such as I/O cards, firmware, software installed, and control strategies. Detailed configuration information gives engineers and cybersecurity personnel the same view of data, which translates into more consistent, coordinated, and speedier decisions — important capabilities when the goal is to prevent potential plant upsets or harm to personnel. Finally, the costs to maintain an inventory can decrease by as much as 90% as Inventory in Depth relies on automated data gathering; depending on the frequency, an evergreen inventory is also achievable.

Criticality, priority, and interdependency. Not all cyber assets have the same risk profile in light of plant processes. Therefore, when an unauthorized change happens on a critical asset, such as a safety instrumented

system (SIS), the incident- response protocol will have different steps and degrees of urgency than protocols for other systems, such as a data historian. Discriminating between cyber assets means having a method of categorizing the systems so that each can receive appropriate scrutiny and responsiveness if an incident occurs.

Since few systems act independently in a plant, it is also important to understand how systems are related to each other. Should the system go down due to a cyber attack or engineering mistake, personnel can make better recovery decisions based on knowing what other systems are affected. Having this information is a good engineering practice that also allows cybersecurity personnel to better manage risk across the entire enterprise.

New device discovery. While a simple "ping sweep" will identify new assets on a network, finding new or changed proprietary cyber assets relies on a different tactic — digging into the configuration files of proprietary systems and finding system references that are not currently inventoried. Once an asset is recognized, cybersecurity or engineering personnel should ideally receive notifications of a new device, as well as missing ones (for instance, those resulting from a system upgrade). Then, established workflows can guide them through the process of updating data imports, policies, processes and other cybersecurity functions.

Enabling new usage scenarios

An OT and IT inventory opens up new ICS cybersecurity use cases that were previously unavailable or difficult to achieve. Cybersecurity and operations personnel can now perform the following tasks:

1. Identify exposure to published vulnerabilities

Scenario: ICS-CERT (Box, p. 62) [2] published a critical vulnerability advisory in early 2015 concerning multiple models and versions of a specific transmitter. This transmitter works across any manufacturer's control system and not just the manufacturer's. The advisory describes the vulnerability as critical, noting that it has the potential to impact operations if left unaddressed.

Solution: If a comprehensive OT inventory exists, a simple query will immediately identify every control system that has this transmitter. Only an inventory that spans the heterogeneous, proprietary control systems in a plant will provide complete results. Once the situation is remediated, to prevent future occurrences of this vulnerability, an automated policy can look for and flag instances of when that same transmitter is reintroduced into the control environment (for example, through the spares inventory).

2. Unauthorized change to a control strategy

Scenario: An engineer connects to a particular safety system to make a simple change. The engineer mistakenly removes the ability for the operator to recognize the availability of that safety system.

Solution: Inventoried configuration data are analyzed for changes, with unauthorized changes flagged for

investigation. An incident-response protocol drives remediating actions needed to restore the safety system. The next data import captures evidence that the safety system's configuration was properly restored.

3. Preparing for the inevitable breach

Scenario: Hackers gain access to systems in Level 1 and below. A multi-threaded attack includes firmware updates to serial-to-Ethernet devices, similar to the Ukrainian power plant hack carried out in December 2015.

Solution: Change detection utilizing a security baseline will surface the malicious firmware updates, and change management procedures and automated workflows will drive needed actions. If a worst-case scenario occurs, automated backups taken during the Inventory in Depth process will speed recovery, as part of a comprehensive disaster recovery plan.

Today, the majority of CPI operating companies cannot effectively execute these three use cases. Where they stumble is not having an accurate, comprehensive inventory of all their cyber assets, which hinders swift, consistent action when these security policies are violated.

A comprehensive solution

A best-in-class inventory management solution deciphers and integrates control-system configuration data from both proprietary and non-proprietary systems into a single repository. Such a solution detects new or missing devices, provides a facility for asset classification, enables appropriately leveled incident response protocols, and accurately captures system interdependencies in sufficient detail.

An automated, normalized inventory data across all major IT and OT assets in the control network presents a holistic view of control system assets — beyond the reach of traditional manual, vendor-supplied, or IT-only solutions. Plant personnel monitor and detect unauthorized changes centrally and then investigate, remediate, and mitigate through automated policies and workflows. The result is greater operational efficiency, improved audit capabilities for compliance, closed-loop patch-management processes, and a speedy recovery in the event of a lost production system. ■

Edited by Suzanne Shelley

References

1. Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), 2014 Industrial Control Systems Assessments Overview and Analysis, Accessed online at: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2014_Year_End_Assessment_Report_S508C.pdf
2. https://ics-cert.us-cert.gov/advisories/ICSA-15-029-01

Author

David Zahn is chief marketing officer and the general manager of the Cybersecurity Business Unit at PAS (16055 Space Center Blvd, Suite 600, Houston, TX 77062; Phone: 281-286-6565; Email: david.zahn@pas.com). He has more than 24 years of enterprise software and services experience within startup and high-growth companies in the oil and gas sector and IT fields. Prior to PAS, Zahn was vice president of marketing at FuelQuest and vice president of marketing at Avalara. He is a frequent speaker at cybersecurity industry events, and holds a BA in economics and managerial studies from Rice University, and MBA from the McCombs School of Business at the University of Texas (Austin).