DITTA GLOBAL DIAGNOSTIC IMAGING, HEALTHCARE IT & RADIATION THERAPY TRADE ASSOCIATION

DITTA White Paper on Cybersecurity:

Best Practices for Sharing Cybersecurity Information

Executive Summary

Purpose

Best Practices for Sharing Cybersecurity Information identifies industry best practices and guidelines that medical technology manufacturers may consider when providing cybersecurity information to their customers. This information is meant to help customers effectively manage their cybersecurity expectations as they use the equipment within the context of their respective markets. The document also provides suggestions for how manufacturers can work with their customers to improve the customer's level of cybersecurity through industry best practices and guidelines. The guidelines described in this document focus on people, processes, and products.

Document Structure

For each fundamental principle, the following information is provided:

a. Identification of threats and an analysis of their implications;
b. Additional reference documents;
c. Recommendations that medical technology manufacturers may consider when providing cybersecurity information to their customers and:
d. Suggestions for how manufacturers can work with their customers to improve the customer's level of cybersecurity.

CONTENTS

Table

Introduction

This document identifies industry best practices and guidelines that medical technology manufacturers may consider when providing cybersecurity information to their customers. This information is then meant to help customers effectively manage their cybersecurity expectations as they use the equipment within the context of their respective markets. The document also provides suggestions for how manufacturers can work with their customers to improve the customer's level of cybersecurity through industry best practices and guidelines. The guidelines described in this document focus on people, processes, and products.

Document Scope

The document provides guidance on the types and levels of information that the manufacturers can provide to their customers to effectively manage their cybersecurity expectations. This document also addresses raising a customer's level of cybersecurity by following seven fundamental principles:

a. Segmenting networks,

b. Understanding data types and flows,

c. Monitoring devices and systems,

d. User management,

e. Hardening devices,

f. Updating devices, and

g. Providing a recovery plan/escalation process.

This document is not meant to be all-inclusive. It is a representative set of best practices that medical technology manufacturers may consider when providing cybersecurity information to their customers as they utilize manufactured equipment within the context of their respective markets. This document is also not intended to describe security best practices (such as access control and data encryption) for the manufactured devices themselves.

Definitions

Active Directory: Microsoft's trademarked directory service, which is a centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories.

Asymmetric Keys: A cryptography algorithm that uses a public/private key pair for encryption and decryption.

Cyber Hygiene: A reference to the practices and steps for users of computers and other devices to take to maintain system health and improve online security.

Demilitarized Zone (DMZ): A physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet.

Domain Name Server (DNS): The system that automatically translates Internet addresses to the numeric addresses that computers use.

Internet Assigned Numbers Authority (IANA): A nonprofit private American corporation that oversees global coordination of the DNS root zone, assigns IP addresses, and other Internet protocol resources.

ICS-CERT: A component of the U.S. Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) that coordinates security incidents involving control systems, facilitates information sharing, and provides online training programs. (https://ics-cert.us-cert.gov/)

Internet of Things (IoT): The IoT refers to the ever-growing network of physical objects that have internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems.

Internet Protocol (IP): A communications protocol for computers connected to a network, especially the Internet, specifying the format for addresses and units of transmitted data.

Lightweight Directory Access Protocol (LDAP): An application protocol for querying and modifying items in directory service providers like Active Directory.

Managed Security Service Provider (MSSP): An organization that provides outsourced monitoring and management of security devices and systems.

Passphrase: A sequence of words or other text used to control access to a computer system, program, or data.

Remote Authentication Dial-In User Service (RADIUS): A networking protocol that provides centralized authentication, authorization, and accounting management for users who connect and use a network service.

SAFECODE: The Software Assurance Forum for Excellence in Code (SAFECODE) is a nonprofit organization exclusively dedicated to increasing trust in information and communications technology products and services through the advancement of proven software assurance methods. (https://safecode.org/)

Security Information and Event Management (SIEM): A security management approach to provide a holistic view of the security-related information that is collected, correlated, and analyzed.

Service Level Agreement (SLA): A contract between a manufacturer and a customer that documents and defines the services the manufacturer is obligated to provide.

Software Maintenance Agreement: An agreement that provides ongoing software support after its delivery.

Symmetric Key: A cryptography algorithm that uses the same cryptographic keys for both encryption and decryption.

The SANS Institute: A private U.S. for-profit company that specializes in information security, cybersecurity training, and selling certificates. (https://www.sans.org/)

Universal Serial Bus (USB): An industry standard that defines cables, connectors, and communications protocols for connection, communication, and power supply between computers and devices.

Whitelisting: An access control approach based on a list of acceptable entities that are allowed access to a system or network blocking out everything else.

Education

Customer education is one of the most under-invested and under-appreciated aspects of cybersecurity. A key component of implementing cyber hygiene is obtaining a knowledge of cybersecurity fundamentals and increasing awareness of how to practice it. Many educational and training resources can aid in this area, including the SANS Institute (https://www.sans.org/), ICS-CERT (https://us-cert.cisa.gov), and SAFECODE (https://safecode.org/).

Training objectives should be established for customers, including ensuring that personnel are able to perform the following activities:

a. Recognize and report suspected cyber incidents to the proper authority,
b. Understand how to handle and secure sensitive information,
c. Ensure that cybersecurity is on the agenda in staff meetings similar to safety briefings or other important topics which are discussed on a frequent basis, and
d. Undertake cybersecurity training as an ongoing activity throughout the year.

Risk Assessment

Medical technology manufacturers need to ensure that their customers understand that there can be risks to applying cyber hygiene practices to any system. As such, manufacturers need to stress the importance of their customers conducting a risk assessment prior to applying any new policies or incorporating new technologies. Risk assessments allow a customer to understand the systems they have and plan for where they may need additional or compensating countermeasures to address the risks.

Manufacturers should provide information on mitigating different types of potential risks that may be related to their products. The potential risks discussed by the manufacturer need not be a comprehensive list but should relate to some of the use cases that the manufacturer has planned for during product development. By recommending that customers perform a risk assessment and presenting some of the potential risks of applying different policies and technologies, manufacturers can aid their customers in mitigating the risks to an acceptable level.

Manufacturers should also emphasize that customers do not focus strictly upon the device-level risks during the assessment. Some of the major sources of cybersecurity vulnerabilities are systemic and result from integrating multiple devices together into systems. While one manufacturer should not be expected to discuss another’s products, they should make their customers aware that they should pay special attention to the integration points between devices.

If an organization does not have an existing risk assessment framework, some examples are:

a. Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)

   https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=309051

b. Factor Analysis of Information Risk (FAIR)

   https://www.fairinstitute.org/fair-risk-management

c. National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF)

https://www.nist.gov/cyberframework/risk-management-framework

d. Threat Agent Risk Assessment (TARA)

https://itpeernetwork.intel.com/whitepaper-prioritizing-information-security-risks-with-threat-agent-risk-assessment/#gs.9trytf

Risk assessment should take the possible impact on safety into consideration. When dealing with security measures in a healthcare setting, standards such as the ISO/IEC 80001-1 can aid in managing these concerns.

Effectively communicating cybersecurity information to customers

To enable customers to effectively manage their cybersecurity expectations, several types of security relevant information can be provided to them by the manufacturer. This can include, but is not limited to:

a. Security guidance through Instructions for Use.

Note: The instructions for use should address the expectations of security controls present in the customers network (the intended environment of use) and should provide further advice on malware protection, role-based access, backups, and other users responsibilities.

b. Generic Product Security and privacy capability information as captured for instance in the Manufacturers Disclosure Statement for Medical Device Security (MDS2).

c. Security advisories and field safety notifications in case of unmitigated vulnerabilities.

Note: To expedite informing customers, next to providing Field Safety Notifications for security issues, it might be advisable to publish security advisories on the manufacturers website and/or through security organizations such as H-ISAC (https://h-isac.org/) and the Cybersecurity & Infrastructure Security Agency in the USA (https://us-cert.cisa.gov/).

d. Information of security updates and upgrades where the customer is responsible for the security of the platform (e.g. for SaMD).

Note: When the customer is responsible for security updates and upgrades as is the case for some software-only products, then the manufacturer could inform its customers when either patches are compliant or non-compliant with the product.

e. Information about end-of-life / end-of-support, device component obsolescence and transfer of risk.

Note: In general, the manufacturer has the obligation to ensure the product is maintained secure, but this obligation shifts to the customer when the product is declared end-of-life. In such case the manufacturer could provide the customer with more detailed risk information for the continued use of obsolete / unsupported products.

f. Advice for joining security information sharing organizations to attain relevant security information.

Note: Provide advice to customers to join national CERTs, ISACs or other information sharing organizations to quickly learn about relevant security threats.

g. Coordinated Vulnerability Disclosure contact information and other means for the customer to inform the manufacturer about discovered vulnerabilities and get quickly into contact with the appropriate security teams.

Fundamental Principles

For each of the following fundamental principles, this document contains an identification of threats, their relevance (including appropriate informative reference standards or other documents that might apply), an analysis to determine implications, and recommendations that DITTA manufacturers may provide to their customers.

Although the individual recommendations are very valuable, unmanaged security activities might not prove to be very effective or sustainable in an organization. Therefore, healthcare providers should understand the importance of an overall Information Security Management System, such as can be established using the ISO/IEC 27001 standard.

1.Segmenting Networks

This principle focuses on the practice of splitting a computer network into sub-networks (also called zones or sub-nets), each being independent network segments. This provides the capability to segment zones with differing security requirements. Compartmentalizing devices into zones does not necessarily mean isolating them.

Identification of Threats and Analysis of Their Implications

Segmenting networks provides a way for communication through zone boundaries to be monitored and managed. Whether the network traffic is entering (ingressing) or leaving (egressing) the zone, it should represent the minimum communication set necessary to maintain proper operations.

Segmenting networks also provides some protection against the spread of an incident. By limiting the network traffic that can enter or leave a zone, the spread of an incident from one zone to another through a network can be slowed or stopped. This often reduces the consequences of an incident.

Reference Documents

a. IEC 62443-2-1:2010 Industrial communication networks—network and system security—Part 2-1: Establishing an industrial automation and control system security program
    1. A.3.3.4 Network Segmentation
b. IEC 62443-3-3:2013 Industrial communication networks—network and system security—Part 3-3: System security requirements and security levels
    1. SR 5.1 Network Segmentation
c. NIST SP 800-53 Rev 5 Security and Privacy Controls for Information Systems and Organizations
    1. AC-4 Information Flow Enforcement
    2. SC-7 Boundary Protection
d. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
    1. 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
e. NIST SP 800-82 Rev 2 Guide to Industrial Control Systems (ICS) Security (May 2015)
f. NIST SP 800-125B Secure Virtual Network Configuration for Virtual Machine (VM) Protection (March 2016)
g. NIST SP 800-153 Guidelines for Securing Wireless Local Area Networks (WLANs) (February 2012)

Manufacturers Recommendations

Manufacturers should provide network segmentation guidance to their customers, so customers know what to expect when their products are deployed. For example, if the product is designed to be deployed on an industrial network protected from the Internet by one or more firewalls, the customer should be informed of that fact. By providing the customer with a set of expectations, the manufacturer can assist its customers in their design process. Manufacturers can also dissuade their customers from deploying the products in ways that may introduce unnecessary vulnerabilities.

When manufacturers recommend using their devices on segmented networks, they should also provide information to the customer on how to communicate with the products through devices like firewalls. This may mean providing information about recommended deployment methodologies, such as using an intermediate server located in a demilitarized zone (DMZ). Manufacturers should also provide recommendations on specific network ports to open in the firewall to allow communication to flow properly. Table 1 provides an example of how to describe a device's communications characteristics within a network configuration.

Table 1—Example of a Required Network Configuration

Service Name	Description	Protocol	Interface Identifier	Port	Expected Client
Use IANA descriptions wherever possible	Describe the protocol	Typically TCP, UDP, IP	Where a device has more than one interface, provide an identifier	Identify the default ports and configurable range	What is expected to connect the port and for what purpose
HTTPS	Hypertext Transfer Protocol Secure - transporting HTML/JavaScript	TCP	ETH 1	443	The device hosts a web server so that administrative users can connect and configure the device via a Graphical User Interface.
Mbap	Modbus Application Protocol	TCP	ETH 2	502 [1025-32768]	The device responds to Modbus on this port

Another situation that manufacturers should consider when providing network segmentation guidance to their customers is the case where the product is isolated and may not have a connection to the business systems and/or Internet. While this situation can seem desirable as a method to provide more security, it

often introduces other risks by not allowing devices to be updated as frequently or easily and by requiring technology like Universal Serial Bus (USB) drives to be employed that have their own vulnerabilities. The recommendations provided by the manufacturer should include procedures for offline initialization and updating if those functions are supported.

Manufacturers should also consider the possibility that their products will be deployed by a customer utilizing wireless networks, and should plan to adhere to the appropriate guidelines for securing wireless networks. If the manufacturer has specific instructions or precautions related to a wireless deployment of their product, they should inform the customer.

Lastly, manufacturers should consider a deployment scenario involving remote access and/or maintenance of the product. Does the manufacturer have any special capability that allows the product to be accessed remotely by customer operations and maintenance staff? Does the manufacturer have any special capability that allows the device to be remotely serviced and/or maintained by the manufacturer? If so, then these should be communicated to the customer. There should not remain secret backdoors for the manufacturer since they may be found by a researcher or adversary and become a vulnerability. If the customer knows about the capability, then they can plan countermeasures accordingly.

2. Understanding Data Types and Flows

This principle focuses on understanding the applications and network protocols being deployed within a product. Customers should begin their data flow analysis exercise by segmenting their data assets into categories based on sensitivity and protection levels required. This categorization will enable the proper scoping and prioritization of the implementation of risk mitigation techniques. For customers, it is important to understand the origination and endpoints for data as it flows through their network, along with data access roles and privileges. It is also important for customers to know what potential software and network ports they may need to manage and monitor along with the product. From the list provided by a manufacturer, customers can establish a map of authorized data flows for their system. Anything observed outside those authorized data flows represents something that a customer should investigate further.

Identification of Threats and Analysis of Their Implications

Within an industrial network, the amount and types of data sent and received are relatively static. The introduction of atypical data flow patterns could represent malicious activities that could compromise or shut down the network. Within networks where the data is more dynamic, other security techniques must be used to monitor for potential malicious activity, given the lack of typical flow patterns.

Reference Documents

a. IEC 62443-2-4:2015 Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers
    1. SP 03.09 Architecture, Data Protection, Communications
    2. SP 03.10 Architecture, Data Protection, Sensitive Data
b. IEC 62443-3-2 (Draft) Security for industrial automation and control systems—Part 3-2: Security risk assessment and system design
    1. ZCR 6.4 Zone and conduit characteristics
c. NIST SP800-53, Rev 5: Security and Privacy Controls for Information Systems and Organizations
    1. AC-4 Information Flow Enforcement

2. CA-9 Internal System Connections

d. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements

1. 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3

e. NIST SP 800-82 Rev 2 Guide to Industrial Control Systems (ICS) Security (May 2015)

f. NIST Data Flow Software Tools – NIST Data Flow System Version 2 – available for download from - https://www.nist.gov/itl/iad/mig/nist-smart-space-project/nist-smart-space-project-data-flow/data-flow-downloads

g. NIST Data Flow System Version 2 User's Guide – available for download from - https://www.nist.gov/itl/iad/mig/nist-smart-space-project/nist-smart-space-project-data-flow/nist-data-flow-system-ii

Manufacturer's Recommendation

Customers need to understand expected data flows across a particular network. Specifically, as data flows from Point "A" to Point "B" on a network, it might not be appropriate to have it revealed to any other device on the network, or the data itself should not be modified in its format or content. Further considerations need to be addressed if the data is entering a network from an outside source (such as the cloud) through a firewall or gateway.

As a general guideline, data flows across a network should have the following features:

a. **Timeliness:** The data should be transmitted in a limited and controlled time frame.

b. **Accuracy:** Changes shouldn't be made while data is being transmitted.

c. **Delivery:** The data should only get delivered to its intended user.

In addition to explaining network segmentation per section 0, manufacturers also should explain to their customers the applications and network ports that come with the product. In some cases, such as products based upon Microsoft Windows, there may be applications installed on the product not directly associated with the manufacturer's desired product functionality. These may provide additional capabilities for the customer, but it may be outside of the control of the manufacturer.

Manufacturers often provide additional network functionality in their products beyond the minimum set needed to operate correctly. For example, a product may have an embedded web server to provide diagnostic information. The web server is not part of the core functionality of the product but provides a benefit to the customer when operating and maintaining the product. Manufacturers need to ensure that customers are aware of the additional functionality that is accessible from the network to allow them to weigh the risks and benefits of that functionality.

3. Monitoring Devices and Systems

Customers are ultimately responsible for monitoring the devices and systems on their network. Manufacturers should provide the capability for customers to monitor their devices, preferably using some centralized monitoring technology.

In addition to simply monitoring the devices and systems on their network for potential security incidents or anomalies, customers may expect that manufacturers' products are able to report identifying information. This allows customers to accurately inventory their devices and systems. Being able to centrally collect that information may obviate touching each device or system.

Collecting and analyzing the information from these devices provides an early indication of an atypical event.

One mechanism that manufacturers can utilize to provide device security information to customers is the Software Bill of Materials (SBOM). The SBOM is a maintained list of software components utilized in a device or system and can assist in detecting potential security threats by identifying software component at risk. A typical SBOM contains component information such as component vendor, component name, and component version. The SBOM should be updated as software components are upgraded or changed.

Identification of Threats and Analysis of Their Implications

An effective monitoring system will serve to enhance the built-in security of the corresponding device or system.

Reference Documents

a. IEC 62443-3-3:2013 Industrial communication networks—Network and system security—Part 3-3: System security requirements and security levels
    1. FR 6 Timely response to events
b. NIST SP 800-53 Rev 5 Security and Privacy Controls for Information Systems and Organizations
    1. AU-2 Audit Events
    2. AU-3 Content of Audit Records
    3. AU-7 Audit Reduction and Report Generation
    4. AU-8 Time Stamps
    5. CA-7 Continuous Monitoring
    6. SI-4 System Monitoring
c. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
    1. 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 9.1, 9.2, A.12.4.1, A.12.4.4, A.18.2.2, A.18.2.3
d. NIST SP 800-82 Rev 2 Guide to Industrial Control Systems (ICS) Security (May 2015)
e. IETF RFC 5424: The Syslog Protocol
f. FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices
g. FDA Postmarket Management of Cybersecurity in Medical Devices

Manufacturers Recommendation

Customers may want to maintain an inventory of all the devices on their network, identifying items such as vendor, model number, serial number, and firmware revision. Manufacturers can provide some of this information to their customers by supplying, for example, an SBOM with their device. Manufacturers

should educate their customers about how to retrieve that information, especially if it is available through a central server. This will aid the customer to automatically generate and maintain an accurate asset list, an essential part of monitoring and detecting incidents.

Manufacturers that build products with the ability to monitor them from another location (such as a central monitoring system) should describe the events and alerts that the product can generate. The protocols used to communicate alerts and events should be able to assign different levels, priorities, or identifiers. Manufacturers should provide context around these alerts and events for their customers, such as end-point protection alerts, blocked firewall egress attempts, and adding new administration users. They should explain the difference between informational events and warnings so that customers can understand and utilize them in their alarm management and incident response plans.

Customers are often challenged with integrating devices into their monitoring environment while lacking a clear understanding of the kinds of events, alarms, and statistics that a particular device or component can generate. Manufacturers can ease integration of their products into a customer monitoring environment by documenting the events, alarms, and statistics that the product generates and by explaining the relative criticality of the information. A clear explanation of the information, its meaning, and implication to a customer, and a recommended customer action when a given event occurs can be used by customers to be more prepared and informed. Clear and concise documentation of events and statistics will increase the chance that the customer will achieve the desired response. Where possible; events and alarms should also include succinct textual recommendations on actions that a customer should take in response to the event.

Devices on the network should be monitored to determine how they typically interact. A Security Information and Event Management (SIEM) tool can provide many capabilities and services for customers to efficiently provide a holistic view, not only into a particular network infrastructure, but also its workflow, compliance, and log management. At its core, a SIEM provides event and log collection, layered centric views, normalization, correlation, adaptability, reporting and alerting, and log management. Customers may not have the expertise to deploy and manage a SIEM on their own. In that case, Managed Security Service Providers (MSSP) can often provide turn-key solutions.

4. User Management

Manufacturers should provide user management capabilities to their customers so they can intelligently control access to their computer network. User management typically covers the following four areas:

a. **Administration—**Users designated as administrators should have the capabilities to create, modify, and delete accounts on the system. This could be either centrally or locally managed.

b. **Authentication—**There should be a process to verify the identity of a user. Based on the degree of acceptable risk, this could be multi-factor.

c. **Authorization—**The capability should be provided to manage user privileges, for example, role-based access control.

d. **Audit—**There should be a way to monitor the actions taken and resources consumed by a user or process, and to store this data in an audit log.

Identification of Threats and Analysis of Their Implications

Perhaps one of the most common threats is manufacturers not enforcing a mandatory default password change during the initial configuration of a product. While default passwords are very useful for manufacturers and customers in allowing quick configuration of a device from its out-of-box state, issues arise when default passwords are not changed by the customer, manufacturers do not provide an easy mechanism to change them, or hard-coded passwords are included in the product.

When a customer returns a device for maintenance, and they have assigned it a unique password, it may be difficult for a manufacturer to retrieve product performance and activity logs that are needed for the repair process.

Reference Documents

a. IEC 62443-2-1:2010 Industrial communication networks—Network and system security—Part 2-1: Establishing an industrial automation and control system security program
    1. A.3.3.5 Element: Access Control: Account Administration
    2. A.3.3.6 Element: Access Control: Authentication
    3. A.3.3.7 Element: Access Control: Authorization
b. IEC 62443-3-3:2013 Industrial communication networks—Network and system security—Part 3-3: System security requirements and security levels
    1. Support of essential functions
    2. FR 1 Identification and authentication control
    3. FR 2 Use control
c. NIST SP 800-53 Rev 5 Security and Privacy Controls for Information Systems and Organizations
    1. AC Access Control Family
    2. AU-14 Session Audit
    3. IA Identification and Authentication Family
d. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements
    1. 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.6.2.1, A.6.1.2, A.6.2.1, A.6.2.2, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.4, A.9.4.5, A.11.1.5, A.11.2.6, A.11.2.8, A.11.2.9, A.12.1.1, A.12.4.1, A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3, A.18.1.1, A.18.1.3, A.18.1.5, A.18.2.2
e. NIST SP 800-82 Rev 2 Guide to Industrial Control Systems (ICS) Security (May 2015)

Manufacturer Recommendation

While manufacturers' products may provide the capability to manage users, it is up to the customers to implement those capabilities properly to maintain the security of those products. Manufacturers should make recommendations to their customers about implementation strategies and advise them on user management.

Manufacturers can assist their customers in implementing user management by providing use cases that involve the full life cycle of a user. This would allow the manufacturer to provide recommendations on

integrating the hiring process with the ability to create and manage users with their product. It could also discuss modifying a user's role-based upon a job change and eventually disabling and deleting user accounts due to leaving their position. It would also allow the manufacturer to highlight and distinguish their functionality, such as providing for greater granularity in user role management or distinctions between 3rd-parties and/or contractors from normal operators and engineers.

A common security recommendation for customers is that they audit their user accounts on a regular basis. If a manufacturer has implemented the capability to audit user accounts on their products, they should make their customers aware of how to use this auditing capability. This will greatly increase the customer's ability to monitor their user accounts with less time spent collecting the data.

Internet of Things (IoT) devices have proliferated, and some have posed a threat to the Internet at large. This is because of the sheer number of IoT devices and because some manufacturers of these products have not taken appropriate cybersecurity measures to protect them. As a result, IoT products have been compromised and used for malicious purposes. One typical way devices have been compromised is through default passwords, which customers often do not change and frequently aren't even aware exist.

Default passwords are typically used to perform initial commissioning of the device because known defaults simplify the process. It is recommended that manufacturers require that default passwords be changed before the device becomes capable of communicating operationally. Password complexity requirements vary by industry. Manufacturers are encouraged to prevent the user from using weak passwords by conforming to these password complexity standards. Typically, a device will have one or more locally stored accounts and/or passwords to perform various functions when central remote user authentication and authorization is not available or enabled.

Inevitably, passwords for local authentication will be lost or forgotten. The following are recommended best practices for the recovery of such a device:

a. Whenever possible, centrally authenticate (e.g., via RADIUS, LDAP, or Active Directory) a user as a privileged security administrator of the device. Also, permit the privileged user to reset local account passwords to a new value.
b. When central authentication is not possible, manufacturers should provide some mechanism that is not network-based, for example, a reset button or special power-on sequence, to reset a device to its default configuration and/or password thereby allowing customers to restore access to the device. Manufacturers should document reset mechanisms clearly so that customers understand the operational state of the device prior, during, and after the reset process.
    1. The user should be required to change the default password as part of the password reset process in much the same way as is required for initial commissioning of the device.
    2. When a device is reset, it should communicate the reset operation to a logging service or system.
    3. Safe operation of the device should continue while the user is resetting the password.
    4. The system should delete any sensitive customer information stored in the device after a password reset has occurred. The system should securely wipe cryptography keys, certificates, and IP addresses or DNS names stored in the device to prevent disclosing private customer information.

5. Manufacturers should provide a means to back-up a device's configuration and settings and enable the restoration of the configuration and settings after a password reset has occurred in order to bring a device back into fully operational state with minimal downtime.

Manufacturers sometimes overlook product return maintenance. Devices that are correctly hardened, and password protected with customer passwords, should otherwise prevent access to the information needed by manufacturers to diagnose problems. The following best practices are recommended:

a. Manufacturers should document their customer data privacy policy regarding the information that they can retrieve from a returned device.

b. The mechanism used by the manufacturer to recover diagnostic information, logs, and configuration settings from the device should not include the recovery of personal information, including symmetric and asymmetric keys, certificates, passphrases, etc.

c. When a device is accessed by the manufacturer for maintenance, the device should wipe all sensitive customer data but preserve and allow the manufacturer to access diagnostic data.

d. A device that is accessed by a manufacturer should be fully reset before being returned to service.

e. The method used by the manufacturer to gain access to diagnostic information should require physical access to the device and may be a variation of the process used by customers to recover from lost or forgotten passwords.

5. Hardening Devices

This principle addresses techniques manufacturers provide to their customers to harden devices based on the requirements of a particular market.

Identification of Threats and Analysis of Their Implications

As equipment manufacturers provide their customers with more effective network defenses, attackers identify alternate methods to enter the protected and trusted network environment. Once inside, these attacks can exploit vulnerabilities or compromise the environment using multiple vectors such as web, email, and malicious files.

One must consider maintenance and functionality tradeoffs when hardening a device. For example, closing network ports or disabling functionality in an operating system could make it harder for a network administrator to complete his/her responsibilities.

For many medical devices, hardening a device after its deployment without the manufacturer's explicit involvement is prohibited.

Reference Documents

a. NEMA CPSP 1-2015 Supply Chain Best Practices

b. NEMA/MITA CSP 1-2016 Cybersecurity for Medical Imaging

c. IEC 62443-3-3:2013 Industrial communication networks—Network and system security—Part 3-3: System security requirements and security levels

   1. SR 3.5 Input validation

   2. SR 3.6 Deterministic output

3. SR 3.7 Error handling
4. SR 4.3 Use of cryptography

d. NIST SP 800-53 Rev 5 Security and Privacy Controls for Information Systems and Organizations
   1. SC-27 Platform-Independent Applications
   2. SC-41 Port and I/O Device Access

e. ISO/IEC 27001:2013
   1. 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.9.1.1, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.6, A.12.1.1, A.12.2.1, A.12.5.1, A.12.6.2, A.13.1.1, A.13.1.2, A.13.1.3, A.14.1.1,

f. NIST SP 800-82 Rev 2 Guide to Industrial Control Systems (ICS) Security (May 2015)

Manufacturer Recommendations

Manufacturers should provide their customers with devices which are secure by default and provide procedures for hardening their devices if they provide that capability. The procedures for hardening should also allow for some functions to be hardened, while others remain open to accommodate different customer environments.

Manufacturers also need to provide some of the risk trade-offs to their customers when hardening their products. In most cases, hardening involves disabling certain product functions or installing endpoint protection. If a customer chooses to implement the hardening procedure, they should be informed about the impact on the functionality and risks if not configured correctly. This will help the customer make a risk-based decision on whether to implement the hardening procedure or not.

There are some instances where a manufacturer may not be allowed to harden a device after its installation. In those cases, manufacturers may decide to provide mitigating controls (also known as compensating countermeasures), such as disabling a vulnerable service or disabling ports on the device itself. Manufacturers may also provide a list of recommended and validated endpoint protection software with exact details on how to configure it for the device.

Finally, manufacturers should make their customers aware of any safety and warranty implications should a customer harden one of their devices. While physically disabling a USB port on a motherboard renders it non-functional, it could also make it non-repairable.

6. Updating Devices

This principle focuses on procedures that manufacturers provide to their customers to update deployed devices after new vulnerabilities have been discovered or when the security requirements and needs of their operating environment have changed.

Updating devices and systems where possible is an important step in keeping up with recent functionality and security improvements.

Reference Documents

a. HIMSS/NEMA HN_1_2019 Manufacturer Disclosure Statement on Medical Device Security

b. NEMA CPSP 1-2015 Supply Chain Best Practices

c. NEMA/MITA CSP 1-2016 Cybersecurity for Medical Imaging

d. IEC 62443-2-1:2010 Industrial communication networks—Network and system security—Part 2-1: Establishing an industrial automation and control system security program

   1. A.3.4.2.5.1 Patching IACS Devices

   2. A.3.4.3 Element: System development and maintenance

e. IEC TR 62443-2-3:2015 Security for industrial automation and control systems—Part 2-3: Patch management in the IACS environment

f. NIST SP 800-53 Rev 5 Security and Privacy Controls for Information Systems and Organizations

   1. MA Maintenance Family

g. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements

   1. 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.11.2.4, A.11.2.5, A.12.1.1, A.18.1.1, A.18.2.2

h. NIST SP 800-82 Rev 2 Guide to Industrial Control Systems (ICS) Security (May 2015)

i. NIST SP 1800-24 (2020) Securing Picture Archiving and Communication System (PACS)—Cybersecurity for the Healthcare Sector

Recommendations to Customers

Updating devices and systems is a common countermeasure discussed in nearly all security standards, guidelines, and recommendations. Depending on the level of risk transfer and existing service agreements, responsibility for updates can fall to the customer or to the manufacturer. There are also risks associated with customer installation of nonvalidated updates (for instance, when a third-party update is automatically transmitted or received).

When customers take part in installation of security updates, they should be made aware of the update processes which determine:

- Applicability: What update shall be deployed to which device?
- Preparation: How should the update be installed, and should application data be archived?
- Scheduling: When should the update be installed and who shall perform the update?

Applicability: Updating processes should be based on a review of a customer's existing asset inventory and contain items such as programmable electric devices, communications gateways, intelligent sensors, and test equipment. This asset inventory should also identify devices that are independently updatable and devices that depend on validated updates from the manufacturer.

Preparation: As cybersecurity is a shared responsibility between different actors (manufacturers, operators, etc.), it is important that efficient mechanisms are in place to ensure that patches are made available after a vulnerability has been detected. Before customers upgrade the operating system or change other software on customer deployed servers or hardware, the customer should coordinate with the manufacturer to ensure that the manufacturer's application software and databases have been tested and are compatible with the proposed customer upgrade. Some manufacturers may offer a Software Maintenance Agreement service, which includes testing and verification services. Archiving application data—especially private health information—may be part of comprehensive updating plans.

Schedule: Manufacturers often provide the capability to update their devices, but customers do not always implement the updates within a timely manner. Customers, in many cases, will weigh associated risks of outdated software against the lost time, lost revenue, and potential downtime to implement the update or the possibility of the update causing a failure.

Recommendations to Manufacturers

Manufacturers need to provide information to their customers on how to apply updates at different times: during operation, planned downtimes, shutdowns, etc. Manufacturers who provide updates to their customers need to inform their customers about the priority of implementing the update. That priority should not always be critical. Manufacturers should provide some context for the update and other measure of the priority from their point of view. This is especially true when a manufacturer embeds 3rd-party libraries or software that requires updating. Manufacturers often need to review the update from their 3rd-party supplier, evaluate the priority provided by that supplier in the context of their device, and then translate it into a priority that accurately reflects any new risk posed by the device.

The sharing of costs will depend on the legal requirements of different jurisdictions, warranty provisions, and the contractual arrangements between manufacturers and operators. Each manufacturer may have different systems in place to establish and cost servicing.

In general, if a patch mitigates a potential impact on safety or performance then the patch should be made available by the manufacturer and in a timely fashion. Other aspects should be addressed in service contracts between manufacturers and operators. Provisions could include:

- Patch management services (e.g., installing patches on a system for the customer);
- Availability and cost of remote servicing;
- Timing and frequency of patch validation (including availability and costs of expedited service).

Manufacturers should also address legacy devices and systems which have been left in the market as they are able. Sometimes such devices are too old to receive patches for new vulnerabilities because of the software or hardware architectures, such as the end of support for third-party components. Manufacturers should monitor the support plans of third-party vendors and provide appropriate information to customers.

Furthermore, manufactures should provide any plans to end support for the device or device components in a timely manner. The plan should include the timeline toward the end of the support including options such as upgrade or replacement information. In addition, the plan may include additional technical information for the continued use of the devices and systems, such as hardening the devices, even though it may present some of the risk trade-offs described in section 5.

Manufacturers should also communicate that third-party component vulnerabilities are not necessarily exploitable in the context of a particular device, and that a new vulnerability does not necessarily constitute a risk to safety or performance of the medical device. Through their updated risk analysis, manufacturers are in the best position to evaluate residual risk and inform their customers accordingly.

In the case that vulnerabilities in third-party components are relevant, but no patches are available, device manufacturers should inform their customers about technical or organizational mitigations.

7. Providing a Recovery Plan/Escalation Process

This principle focuses on providing a recovery plan and an escalation process that customers should use to be able to quickly recover from a malfunctioning or nonfunctioning device which could be caused by a malicious attack or an incident on the network.

Identification of Threats and Analysis of Their Implications

The absence of a recovery plan and escalation process can disrupt business operations, information security, IT systems, employees, customers, upstream suppliers, and other vital functions.

Reference Documents

a. NEMA CPSP 1-2015 Supply Chain Best Practices

b. IEC 62443-2-1:2010 Industrial communication networks—Network and system security—Part 2-1: Establishing an industrial automation and control system security program

    1. A.3.4.5 Element: Incident planning and response

c. IEC 62443-3-3:2013 Industrial communication networks—Network and system security—Part 3-3: System security requirements and security levels

    1. SR 7.3 Control system backup

d. NIST SP 800-53 Rev 5 Security and Privacy Controls for Information Systems and Organizations

    1. IR Incident Response Family

e. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements

    1. 5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.7.2.2, A.12.1.1, A.16.1.1, A.16.1.2, A.16.1.4, A.16.1.5, A.16.1.6, A.18.1.1, A.18.2.2

f. NIST SP 800-82 Rev 2 Guide to Industrial Control Systems (ICS) Security (May 2015)

g. ISO/IEC 29147:2014: Information Technology—Security Techniques—Vulnerability Disclosure

h. ISO/IEC 30111:2013: Information Technology—Security Techniques—Vulnerability Handling Processes

i. NIST Cybersecurity Framework V1.1

Manufacturers Recommendation

Managing and responding to incidents and disaster scenarios is up to the customers. Customers need to have properly designed incident response plans, disaster recovery plans, and business continuity plans and execute them accordingly. Manufacturers can provide the capability for instance for backup and recovery and to incorporate the monitoring and alerting functionality inside their product with centralized monitoring systems, but customers are responsible for implementing those capabilities and procedures.

Manufacturers should provide their customers with information on how to receive technical support in case a customer needs assistance with an incident or disaster scenario. This information may be specified as part of a service-level agreement (SLA), but it should be clearly stated how a customer is expected to contact the manufacturer for support. This information should describe the information the manufacturer may ask the customer to supply so they can help them respond to the incident.

Manufacturers should also provide a mechanism for customers and researchers to provide feedback and vulnerability reports on their products. It is not uncommon for customers to discover vulnerabilities in products that need to be fixed. Manufacturers should have a mechanism for customers to submit vulnerability reports securely and customers should be provided with information on how the submission of such information can be accomplished. Similarly, security researchers may find vulnerabilities in products. Manufacturers should provide a mechanism, possibly the same one as for customers, for other interested parties to report vulnerabilities in products. When manufacturers learn of a vulnerability, they should work with the customer and/or researcher to responsibly disclose that information to all their customers. Manufacturers should identify, assess, and share vulnerability information irrespective of where this information comes from. Manufacturers should use plain language, at an appropriate reading

level for the intended user, to communicate actionable information regarding product cybersecurity vulnerabilities and threats. It may be beneficial for the user to include information about the benefits and risks associated with deploying an update, or compensating controls required until the update is available. While this won't eliminate the possibility of an individual releasing vulnerability data about the manufacturer's product without responsible disclosure, it reduces the likelihood of it happening if dealt with responsibly by the manufacturer.