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

DITTA White Paper on Cybersecurity:

Best Practices in the Medical Technology Manufacturing Environment

Preface

Cybersecurity management of production and engineering processes, as categorized within the scope of this document, can have a positive impact throughout medical technology organizations.

DITTA believes that the number of cybersecurity requirements within the medical technology manufacturing facility and engineering processes will increase along with product quality demanded by global regulatory requirements.

Many risks related to cybersecurity can be expected in manufacturing facilities, such as:

- Shutdown of the manufacturing facility and loss of productivity
- Quality loss by the failure of product inspection
- Leak of customer, design, and production engineering information
- Infection of new products with malicious software during production
- Leak of product software certificates

It is constructive and reasonable for stakeholders to discuss the development process of secure medical technology and to share information with healthcare providers. However, this document focuses primarily on the secure environment of the manufacturing facility and engineering processes as another significant challenge for manufacturers.

In this document, “device” refers to any device within the manufacturing facility network, and is not restricted to medical technology products, given the inherent risk in manufacturing facility networks and engineering processes.

The DITTA White Paper on Cybersecurity of Medical Technology is derived from NEMA CPSP 2-2018 Cyber Hygiene Best Practices. Reprinted by permission of the National Electrical Manufacturers Association.

Executive Summary

Purpose

This white paper identifies a set of industry best practices and guidelines that medical technology manufacturers can implement to raise their level of cybersecurity sophistication in their manufacturing facility and engineering processes. This document provides guidelines for proactive and reactive security with a focus on people, processes, and systems.

This document addresses ways to raise a manufacturer's level of cybersecurity sophistication by following seven fundamental principles:

1. Segmenting Networks
2. Understanding Data Types and Flows
3. Hardening Devices
4. Monitoring Devices and Systems
5. User Management
6. Updating Devices
7. Providing a recovery plan/escalation process

This document is not meant to be all-inclusive, but rather a representative set of best practices that manufacturers can implement both in their manufacturing facility and engineering processes. This document is also not intended to describe security best practices for organizations that implement the manufactured devices. Finally, this document does not explicitly consider the unique security needs of Health IT service providers, although some of the guidelines provided may be applicable to those businesses.

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, and;
c. Recommendations that medical technology manufacturers should incorporate.

Table of Contents

Introduction

This cybersecurity document identifies a set of industry best practices and guidelines for medical technology manufacturers to raise the level of cybersecurity sophistication in their manufacturing facilities and engineering processes. This document provides guidelines for proactive and reactive security with a focus on people, processes, and systems.

The identified practices in this document should be incorporated as part of a broader Security Management effort. Additional information about Security Management can be found in such standards and frameworks as IEC 62443-4-1, the ISO/IEC 27000 series, and the NIST Cybersecurity Framework.

Document Scope

This guideline document addresses raising a manufacturer's level of cybersecurity sophistication by following seven fundamental principles:

1. Segmenting Networks
2. Understanding Data Types and Flows
3. Hardening Devices
4. Monitoring Devices and Systems
5. User Management
6. Updating Devices
7. Providing a Recovery Plan/Escalation Process

Fundamental Principles

For each of the following fundamental principles, the document sections contain 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 should incorporate. The best practices that are described in this document are applicable to most manufacturing environments. Each fundamental principle is useful for manufacturer's cybersecurity activity and can work effectively even when a single principle is implemented.

Segmenting Networks

This principle focuses on the design of data networks that logically/physically separate manufacturing systems data flows from business or public networks. It also provides the capability to segment critical manufacturing sub-networks from other manufacturing sub-networks with differing security requirements. Network segmentation involves dividing the network into smaller networks called zones.

Compartmentalizing devices into zones does not necessarily mean isolating them. Conduits connect the security zones and facilitate the transport of necessary communications between the segmented security zones. Figures 1 and 2 depict a typical segmented manufacturing network (called OT network) as well as a typical segmented multi-institution manufacturing network.

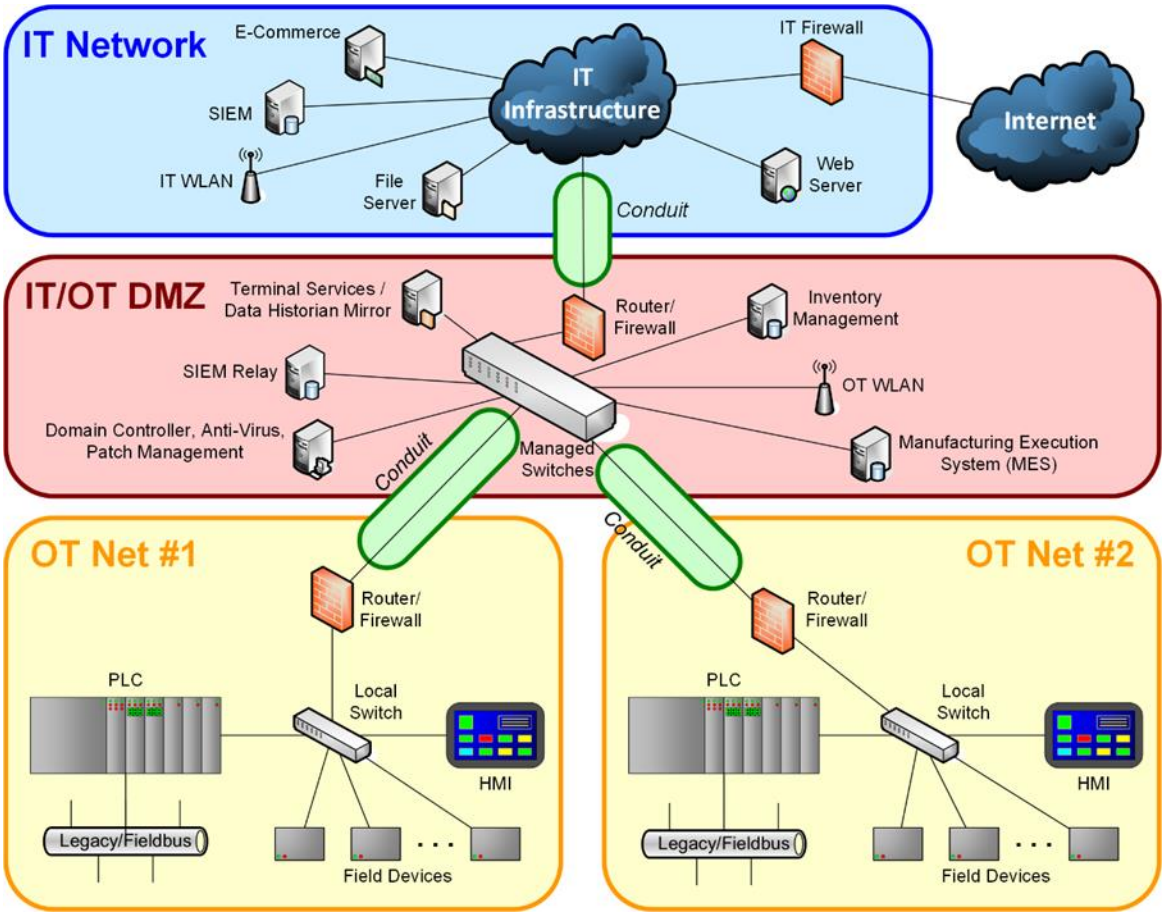

Figure 1. A Typical Segmented Manufacturing Network

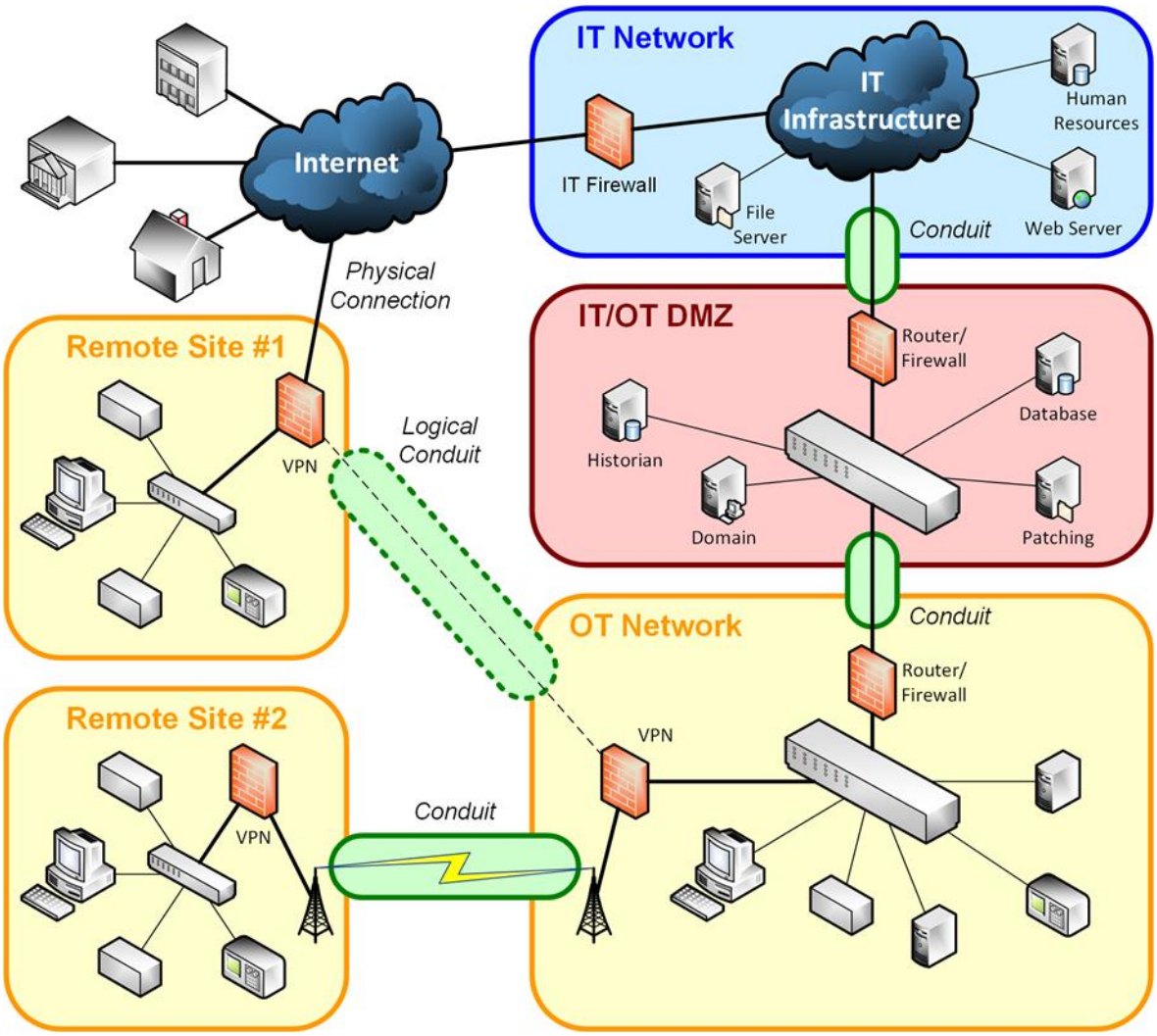

Figure 2. A Typical Segmented Multi-Institution Manufacturing Network

Identification of Threats and Analysis of Their Implications

Through the use of comprehensive risk assessments, manufacturers can identify threats to their devices/solutions. There are many risk assessment methodologies available for manufacturing organizations to use. One of the goals of the segmentation of networks is preventing non-essential or even malicious network traffic from ingressing the operational technology (OT) network. This type of traffic can disrupt, and in some cases, even modify the OT traffic or OT device functions. Therefore, only valid, authenticated OT network traffic should be permitted to enter the OT network zones.

Another goal of the segmentation of networks is to prevent sensitive data from egressing a security zone. Some of the recent high-profile attacks included a “phone-home” capability, where the attack included an exfiltration agent that was able to send data out of the victim’s network back to a command and control host. Again, only valid, authenticated network traffic should be permitted to exit the security zones.

Recommendations for Manufacturers

Networks are segmented through the use of a barrier device that can control what passes through the device. On Ethernet-based networks running the transmission control protocol/internet protocol (TCP/IP), the most common barrier devices in use are firewalls, routers, data diodes, and layer 3 switches.

The generally accepted good practice is to use a barrier device to manage the communication across the conduit that links the OT zone to the information technology (IT) zone. The barrier device can serve as a good automated tool to enforce that security practices be followed in the OT zone, such as not allowing inbound email or communications to/from the Internet.

For high-risk industrial control systems (ICS), the use of a demilitarized zone (DMZ) in conjunction with an OT zone offers additional risk reduction opportunities between the low-security level IT zone and the high-security level OT zone. The security level for the DMZ is higher than the IT zone but less than the OT zone. The function of this zone is to eliminate or greatly reduce all direct communication between the OT zone and the IT zone. Where wireless local area network (WLAN) access to an OT network is considered necessary by a manufacturer, it is recommended that the OT WLAN network have a distinct SSID. The connectivity from that WLAN should be limited to the smallest OT zone possible.

A further consideration for segmentation is that of remote access. Remote access to the OT zone should only be enabled when necessary and authenticated. Remote user access to the OT zone may require multifactor authentication, depending on the security level requirement.

The risk associated with the ICS may be too great to allow any opportunity for compromise by an external agent. A facility may choose to disconnect all conduits between the OT zone and any other zone. This is a very valid network segmentation strategy for consideration. Facilities choosing to adopt this isolation approach are not automatically eliminating all risk. There may still be much vulnerability that could be exploited locally. Appropriate layers of cyber and physical protection should be employed to address the residual risk remaining after isolation of the OT zone from the IT zone.

Segmenting Networks 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 (Draft) Security and Privacy Controls for Information Systems and Organizations (August 2017)
    1. AC-4 Information Flow Enforcement
    2. SC-7 Boundary Protection

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

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

    1. A.13.1.3 Segmentation in networks

[Note for Reference Documents]

- IEC 62443 series

IEC 62443 series is attracting much attention in the field of medical technology although they are standards for Industrial Automation and Control Systems (IACS) security. One of the reasons these standards are applied to medical technology is that IACS is one of the most advanced and established fields in terms of security. In this document those requirements and technologies can directly be applied without any translation because the scope of application for this document is the manufacturing facility and engineering processes.

- NIST SP Standards

Although National Institute of Standards and Technology (NIST) is an organization under United States Department of Commerce, their standardization activity is wide-ranged, comprehensive and worth being referred to in terms of global perspective. They continuously try to align with international cybersecurity initiatives and standards. For example, NIST has held regular discussions with many nations and regions and has made noteworthy internationalization progress. NIST SP 800-53 provides a catalog of security and privacy controls. It is scheduled to be published in March 2019. NIST SP 800-82 provides an overview of ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks. See the links below.

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft
https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

- ISO/IEC 27001

This is one of ISO/IEC 27000 family standards regarded as Information Security Management System (ISMS) standard which is widely recognized in medical technology field. The application of this standard is appropriate because the requirements set out in this International Standard are generic and are intended to be applicable to all organizations, regardless of type, size or nature. And it is also referred to by IEC 62443-2-1 and NIST SP 800-82.

Understanding Data Types and Flows

This principle focuses on the understanding of the manufacturing environment in which network-connected devices are being deployed. For manufacturers and end users it is important to know what data should flow through a network, where that data typically goes, and what or who should have access to it.

Identification of Threats and Analysis of Their Implications

Through the use of comprehensive risk assessments, manufacturers can identify threats to their devices/solutions. There are many risk assessment methodologies available for manufacturing organizations to use. Within an internet of things (IoT), ICS, and supervisory control and data acquisition (SCADA) network, the amount and types of data that they send and receive are relatively static. The introduction of new communication paths outside the norm of typical data flow patterns could represent malicious activities that could either compromise or shut down the respective network.

Recommendations for Manufacturers

When new communication paths, and changes to existing communication paths, are introduced into a network, alarms should go off to indicate that something may be wrong. These alerts would feed into the manufacturers monitoring devices and systems.

Understanding Data Types and Flows Reference Documents

NIST SP800-53, Rev 5 (Draft): Security and Privacy Controls for Information Systems and Organizations (August 2017)

AC-4 Information Flow Enforcement

CA-9 Internal System Connections

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

NEMA/MITA CSP 1-2016 Cybersecurity for Medical Imaging

DITTA White Paper on Cybersecurity of Medical Imaging Equipment (November 2016)

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

A.13.2.1 Information transfer policies and procedures

[Note for Reference Documents]

DITTA White Paper on Cybersecurity of Medical Technology

The DITTA White Paper sets out the principles of current best practices for manufacturers and suppliers. It describes responsibility for cybersecurity cannot lie with a single stakeholder. Manufacturers and hospital IT departments need to cooperate to implement these approaches. See the link below.

https://www.globalditta.org/media-centre/press-releases/article/new-report-from-ditta-underlines-its-commitment-to-cybersecurity.html

Hardening Devices

This principle addresses techniques manufacturers should use to harden (make more secure) the devices employed to design and manufacture products. The best practices may vary depending on the manufacturer's particular industry.

Recommendations for Manufacturers

There are a number of techniques available to manufacturers for hardening the devices employed to design and manufacture products. Manufacturers should consider either turning off or disabling a number of device features that are not needed or may have inherent security risks. Examples include Joint Test Action Group (JTAG), Telnet, SNMP Versions 1 and 2, and wireless communication.

Manufacturers may consider removing unnecessary programs such as games, and browser plug-ins such as Java. Manufacturers may also consider removing unnecessary services such as print spooler and remote desktop. Also, manufactures may consider disabling cookies.

Ethernet and Universal Serial Bus (USB) port blockers can be effective in blocking network traffic into and out of manufactured devices.

Error handling and input validation capabilities should also be considered. Examples include sanitizing inputs, static code testing, and software bill of materials (SBOM) analysis.

With respect to components and supply chain safety, manufacturers should have a process to monitor suppliers and to easily identify component versions that are included in manufactured products. In addition, manufacturers should have test plans in place that enable a thorough evaluation of each component and newly released versions of those components, before they are integrated into the products. These evaluations should include malware detection analysis, along with standard component quality checks. The whitepaper from NEMA, Supply Chain Best Practices, provides additional details regarding supply chain safety and is listed as a reference document at the end of this section.

Data encryption should be used when the information is confidential and sensitive. Manufacturers need to consider if the data must be encrypted at rest within the device, in transit, when it is in transmission, or a combination of both. This decision depends on the data involved, and if it is highly sensitive data, such as Protected Health Information (PHI), encryption at rest and in transit should be deployed. Integrity protection should be used when information transfer must be reliable and without error.

DDOS (Distributed Denial of Service) attacks occur frequently. Some defenses typically involve the use of a combination of attack detection and traffic classification and response tools. They aim to block traffic identified as illegitimate and allow traffic identified as legitimate. While most firewalls and routers do have capabilities to deny incoming traffic from an outside attacker, they can be easily overwhelmed as the attack becomes more and more sophisticated. Other options available include Intrusion Prevention Systems and the use of application front end hardware to analyze data packets as they enter the system and identify them as priority, regular, or malicious.

Finally, manufacturers may wish to consider a ***secure by default*** method by creating a security baseline for all the products they use, in which configurations are set to be the most secure. A drawback is that these settings may be less backwardly compatible and may require more complex initial configuration making them less user friendly.

Hardening Devices Reference Documents

NEMA CPSP 1-2015 Supply Chain Best Practices

NEMA/MITA CSP 1-2016 Cybersecurity for Medical Imaging

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

SR 3.5 Input validation

SR 3.6 Deterministic output

SR 3.7 Error handling

NIST SP 800-53 Rev 5 (Draft) Security and Privacy Controls for Information Systems and Organizations (August 2017)

SC-27 Platform-Independent Applications

SC-41 Port and I/O Device Access

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

DITTA White Paper on Cybersecurity of Medical Imaging Equipment (November 2016

Monitoring Devices and Systems

This principle addresses how manufacturers should provide the ability to monitor the health and security of their devices and systems within their environment. Monitoring capability should be provided through existing well-known and standard software mechanisms (i.e., Simple Network Management Protocol [SNMP], Syslog) that do not get into specific process parameters.

Identification of Threats and Analysis of Their Implications

Through the use of comprehensive risk assessments, manufacturers can identify threats to their devices/solutions. An effective monitoring system will serve to enhance the built-in security of the corresponding device or system.

Recommendations for Manufacturers

Manufacturers should have devices designed to allow centralized monitoring of their performance, network statistics, core functionality, and security features.

SNMP is widely used as it exposes management data in the form of variables on the managed systems organized in a management information base (MIB), describing the system status and configuration. These variables can then be remotely queried (and in some cases, manipulated) by managing applications. While three significant versions of SNMP have been developed, Version 3 features improvements in performance, flexibility, and security. Therefore, Version 3 should be used or supported. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, and printers.

Syslog is a standard for message logging. It allows separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. A wide variety of devices such as printers and routers use the Syslog standard. It can be used for system management and security auditing as well as general information, analysis and debugging. There are also options available within Syslog to use TCP and Transport Layer Security (TLS) if the manufacturer's environment can support it to ensure reliable and secure delivery of security events.

In Windows, Linux or other Operating Systems, an event log can be used as a record of computer alerts and notifications. Microsoft defines an event as "any significant occurrence in the system or program that requires users to be notified or an entry added to a log."

A manufacturer that implements a Security Information and Event Management (SIEM) solution may use the SIEM to gather information from devices such as servers, routers, switches, Intrusion Detection System / Intrusion Prevention System (IDS/IPS) appliances and firewalls to gather a holistic view of security for their entire network. SIEMs often include event analysis capabilities that can identify active security events by correlating information from multiple sources within the manufacturer's network and presenting them in a more context meaningful presentation format to a manufacturer's IT/OT network security engineering personnel.

Monitoring Devices and Systems Reference Documents

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

FR 6 Timely response to events

NIST SP 800-53 Rev 5 (Draft) Security and Privacy Controls for Information Systems and Organizations (August 2017)

AU-2 Audit Events

AU-3 Content of Audit Records

AU-7 Audit Reduction and Report Generation

AU-8 Time Stamps

CA-7 Continuous Monitoring

SI-4 System Monitoring

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

IETF RFC 5424: The Syslog Protocol

User Management

Basic cybersecurity practice begins with the proper training of end users in an organization, especially those in the development and manufacturing environments. Even the most technically sophisticated cyber-defense system cannot stop people from writing their passwords on a sticky note and displaying the note on their monitor. Beyond training, other end user management capabilities can help control access to computer networks and provide additional security.

End-user training – all new end users should be required to take security training, in addition to refresher courses required for existing end users. There are fundamental security principles that can be easily learned and required training helps reinforce best practices.

Administration—Manufacturers should have the capabilities to create, modify, and delete accounts on the system. This could be either centrally or locally managed.

Authentication—Manufacturers should have a process to verify the identity of an end user. Based on the degree of acceptable risk this could be multi-factor.

Authorization—Manufacturers should provide the capability to manage end user privileges, for example, role-based access control.

Audit—Manufacturers should have a way to monitor the actions taken and resources consumed by an end user or process, and to store the data in an audit log. Audit logs should be periodically reviewed, and depending on the access rights involved, might be reviewed more or less frequently.

Identification of Threats and Analysis of Their Implications

Through the use of comprehensive risk assessments, manufacturers can identify threats to their devices/solutions. There are many risk assessment methodologies available for manufacturing organizations to use. For example, the National Institute of Standards and Technology (NIST) provides a cybersecurity framework, referenced below. Risk assessments do not have to be complex to implement. A lack of solid password policies is perhaps one of the most common threats identified, such as manufacturers not enabling a mandatory default password change on first use. While default passwords are very useful for manufacturers and end users in allowing quick configuration of a device from its out-of-box state, issues arise when default passwords are not changed by the end user; manufacturers do not provide an easy mechanism to change them, or hard-coded passwords are included in the device.

As a recent example illustrates, Internet of Things (IoT) devices have been used to create large-scale botnets that can execute crippling distributed denial of service (DDoS) attacks. The Mirai botnet affected

more than 300,000 IoT devices using default or weak passwords to create nearly 600 Mbps of disruptive internet traffic to all affected sites.

Recommendations for Manufacturers

End-User Training

Require all new end users to complete security training and record successful completion in their Human Resources files

Require all existing end users to complete security refresher training periodically (in most cases, this is annually) and record successful completion in their Human Resources files.

Administration:

Ability to add, modify, and delete any user and corresponding credentials within the system.

Authentication:

Requirement to change default passwords upon the first login

No fixed/hard coded credentials (credentials which you are unable to change such as usernames and passwords) into devices

Storing account information

Ability to store accounts locally

Ability to access centrally stored account systems, such as Active Directory or Lightweight Directory Access Protocol (LDAP)

Ability to use multifactor authentication

Usage of public key infrastructure, especially for remote login

Authorization:

Having role-based access

Pre-defined roles

Ability to create user-defined roles

Having role-based account management

Having different roles for normal users versus administrative roles

Ability to assign arbitrary privileges to roles

Ability to map any user account to any role

Audit:

Ability to record user login/logout along with timestamps

Ability to record files accessed and applications run while logged in

Ability to monitor user-created tasks, including scheduled tasks that don't require an active login session.

Ability to record failed login attempts along with timestamps

Ability to record system configuration changes

User Management Reference Documents

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

A.3.3.5 – Element: Access Control: Account Administration

A.3.3.6 – Element: Access Control: Authentication

A.3.3.7 – Element: Access Control: Authorization

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

Support of essential functions

FR 1 Identification and authentication control

FR 2 Use control

NIST SP 800-53 Rev 5 (Draft) Security and Privacy Controls for Information Systems and Organizations

AC Access Control Family

AU-14 Session Audit

IA Identification and Authentication Family

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

NIST CyberSecurity Framework V1.1

KrebsOnSecurity Hit With Record DDoS, https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos

International Standards Organization (ISO) 27002:2013*, Information technology -- Security techniques -- Code of practice for information security controls*

Monitoring and Updating Fielded Devices

This section focuses on procedures that manufacturers should use to monitor for the latest impactful vulnerabilities and update fielded devices to mitigate against these vulnerabilities.

Identification of Threats and Analysis of Their Implications

Identification of threats is the first category in the NIST CyberSecurity Framework V1.1, and should be viewed by manufacturers as an ongoing process. The threat landscape is constantly shifting, with new threats being introduced continuously. Manufacturers should have processes in place to monitor this threat activity and analyze the potential risk to their organization. There are various tools available to perform this analysis, with an end goal producing a report that can be shared with other organizational functions, so that action may be taken. Updating devices and systems where possible is an important next step in leveraging the knowledge gained through monitoring.. Unfortunately, this often gets delayed for a variety of reasons, such as the lack of resources at the manufacturer or the lack of updates from equipment and software providers. In addition, there are risks that users could install un-validated patches or updates themselves, due to the inherent nature patch distribution.

Recommendations for Manufacturers

Patches have become increasingly important as a methodology for updating programs or new system security threats which appear regularly, especially in online environments. Software and hardware providers typically provide some type of patching system for their deployed products and systems. In most instances, the patching system is not automatic as those providers have a number of recommended procedures they follow to verify the authenticity of the patch, test the patch, provide guidance if a reboot of the system is required, and to notify the end user of the appropriate time frame for patch validation.

In some instances, software and hardware providers may decide to recommend mitigating controls (also known as compensating countermeasures), until patches become available and fully tested and validated. Examples include disabling a vulnerable service or disabling ports (which can be done at either the perimeter or device level).

For some environments, software and hardware providers may provide a recommended anti-virus software package or implement a whitelisting access control approach for mitigating security threats.

Monitoring and Updating Fielded Devices Reference Documents

NEMA CPSP 1-2015 Supply Chain Best Practices

NEMA/MITA CSP 1-2016 Cybersecurity for Medical Imaging

NIST CyberSecurity Framework V1.1

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

A.3.4.2.5.1 Patching IACS Devices

A.3.4.3 Element: System development and maintenance

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

DITTA White Paper on Cybersecurity of Medical Imaging Equipment (November 2016)

ISO/TR 11633-1:2009 Healthcare Informatics – Information security management for remote maintenance of medical devices and medical information systems

Providing a Recovery Plan/Escalation Process

This principle focuses on providing a recovery plan/escalation process that manufacturers should use if a vulnerability is found in a device employed to design and manufacture products. This also includes the possibility of an active exploit against the device. It is critically important for manufacturers to recover to a point beyond the discovered vulnerability, otherwise, the recovery will the manufacturer to experience the vulnerability all over again. For example, if there is a breach due to an embedded component, before recovering affected devices, manufacturers should have a plan to upgrade the embedded component to a secure version that eliminates the vulnerability.

Identification of Threats and Analysis of Their Implications

As is common practice in IT environments to have a Disaster Recovery (DR) Plan, manufacturers need to have an Incident Response Plan for cybersecurity issues. The absence of a recovery plan and escalation process can rapidly disrupt business operations, information security, IT systems, employees, customers, upstream suppliers, and other vital functions. By having a plan in place, manufacturers will have already defined the roles and responsibilities of the team and will have procedures in place to respond in an efficient manner. The NIST CyberSecurity Framework V1.1 details this plan in the Protect section of the document.

Recommendations for Manufacturers

Manufacturers should develop a process to manage incidents and vulnerabilities. Ideally, it should include incident detection and recording, classification and initial support, investigation and diagnosis, resolution and recovery, incident closure, monitoring the progress of the incident resolution, and a communication plan to inform affected parties about the status of the resolution. This Coordinated Vulnerability Disclosure (CVD) process is what helps to ensure that discovered vulnerabilities are mitigated appropriately, and that concerned stakeholders are informed. See NIST CyberSecurity Framework V1.1 for more details.

Manufacturers should also maintain communication channels with end users and upstream suppliers in order to keep abreast of any vulnerability issues and steps to mitigate the issues. There are also numerous sources that provide continuous data feeds and can usually simply involve a subscription to receive the latest updates via email or text message. A quick internet search will uncover the various sources available.

Some software and hardware manufacturers have recently been using what are called “bug bounties” to allow security researchers a way to identify and provide information about a vulnerability to the manufacturer. Before a manufacturer embarks on implementing a “bug bounty” program, it should carefully consider the way in which it reacts to the vulnerability discovery itself, the way in which it reacts to the security researcher, and the way in which it makes the information known to its customers. Companies may want to consider first creating an internal computer security incident response team (CSIRT) where security researchers can report bugs via a responsible disclosure mechanism. This can ensure that they have found a way to mitigate those vulnerabilities before considering paying security researchers for the discovery of those vulnerabilities.

Providing a Recovery Plan/Escalation Process Reference Documents

NEMA CPSP 1-2015 Supply Chain Best Practices

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

A.3.4.5 Element: Incident planning and response

NIST SP 800-53 Rev 5 (Draft) Security and Privacy Controls for Information Systems and Organizations (August 2017)

IR Incident Response Family

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

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

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

NIST CyberSecurity Framework V1.1

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.

Bill of Materials (BOM): A list of the raw materials, sub-assemblies, intermediate assemblies, sub-components, parts and the quantities of each needed to manufacture an end product.

Botnet: A number of internet-connected devices, each of which is running one or more software applications with automated tasks over the internet.

Computer Security Incident Response Team (CSIRT): A concrete organizational entity that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident. The goal of a CSIRT is to minimize and control the damage resulting from incidents, provide effective guidance for response and recovery activities, and work to prevent future incidents from happening.

Cookie: A tiny file that is stored on your computer that contains past browsing information.

Cybersecurity: state of protection of confidentiality, integrity, and availability of all data and software used

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

Distributed Denial of Service (DDoS): An attack that makes an on-line service unavailable by overwhelming it with traffic from multiple sources.

Hardening: The process of securing a system by reducing its surface of vulnerability.

Industrial Control System (ICS): A general term that encompasses several types of control systems and associated instrumentation used for industrial process control.

International Electrotechnical Commission (IEC): An international standards organization that prepares and publishes international standards for all electrical, electronic and related technologies

Internet Engineering Task Force (IETF): The body that develops and promotes voluntary internet standards, in particular, the standards that comprise the internet protocol suite.

Information Technology (IT): The technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data.

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.

Intrusion Detection System / Intrusion Prevention System (IDS/IPS): IDS/IPS refers to technical means used to identify unexpected or malicious activity within a network. IDS will typically notify a security

management application (e.g., SIEM) of a potential intrusion, whereas IPS will automatically block an intrusion once detected.

Joint Test Action Group (JTAG): The common name for the IEEE 1149.1 Standard Test Access Port and Boundary-Scan Architecture. It is a method for testing interconnects on printed circuit boards or sub blocks inside an integrated circuit.

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

Management Information Base (MIB): A formal description of a set of network objects that can be managed thru SNMP.

National Institute of Standards & Technology (NIST): A measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce.

Operational Technology (OT): The hardware and software designated to detect or cause changes in the physical state of a system.

Patch: A piece of software that is used to correct a problem with an operating system or software program.

Print Spooler: A system service in the Microsoft Windows operating system that is responsible for the management of the jobs that have been sent to the printer or the print server of a network.

Remote Access: Any access to a control system from another location.

Remote Desktop: A separate program or feature found on most operating systems that allows a user to access and interact with an operating computer system's desktop. The access occurs via the Internet or through another network in a different geographical location.

Risk Tolerance: Risk tolerance refers to the amount of risk a manufacturer is willing to accept in order to meet strategic objectives. Note: Organizations will have different risk tolerances depending on particular sectors and management. Understanding and documenting the acceptable risk level is critical to establishing the correct processes to deal with those risks.

Simple Network Management Protocol (SNMP): An internet standard protocol for collecting and organizing information about managed devices on IP networks.

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.

Supervisory Control and Data Acquisition (SCADA): A control system architecture that uses computers, networked data communications, and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices such as programmable logic controllers to interface to the process plant or machinery.

Transmission Control Protocol / Internet Protocol (TCP/IP): A suite of communication protocols used to interconnect network devices on the internet.

Transport Layer Security (TLS): A cryptographic protocol that provides communications security over a computer network.

Telnet: A protocol used on the internet or local networks to provide a bi-directional interactive text-oriented communication facility using a virtual terminal connection.

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**.**

Wireless Local Area Network (WLAN): A wireless computer network that links two or more devices using wireless communication within a limited area such as a home, school, computer laboratory, or office building.

About DITTA:

DITTA is the united global industry voice for diagnostic imaging, radiation therapy, healthcare ICT, electromedical and radiopharmaceuticals, representing more than 600 medical technology manufacturers, committed to improving health care and patient outcomes. DITTA was created in 2001 and incorporated in 2012 as a non-profit trade association in order to allow growth and enable partnerships with global organizations. Since its inception, membership has grown significantly, and today counts ten regional associations around the globe amongst its members. In 2015, DITTA granted the NGO status in official relations with the World Health Organization and signed a Memorandum of Understanding with the World Bank in 2016. Visit the DITTA website at http://www.globalditta.org.