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

DITTA White Paper on Cybersecurity of Medical Imaging Equipment[1]

[1] *The DITTA White Paper on Cybersecurity of Medical Imaging Equipment is derived from NEMA/MITA CSP 1-2016 Cybersecurity for Medical Imaging. Reprinted by permission of the National Electrical Manufacturers Association, Medical Imaging & Technology Alliance.*

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

Table of contents

1. Introduction

Medical imaging devices, like all computer systems, are subject to risks their might harm the software, hardware, or data security. As devices become increasingly connected to networks, security risks expand into larger-scale intrusions across digital networks. What have been called cybersecurity incidents may compromise confidentiality, integrity, availability of data and functions in medical devices and could affect the safety of patients.

Advancing cybersecurity measures within healthcare and public health needs a 'whole of community' approach, requiring manufacturers, installers, service staff and healthcare providers to accept shared ownership and responsibility. DITTA seeks to foster a collaborative way of addressing current and emerging threats across the life cycle of imaging devices—from design to installation through end of life.

DITTA strongly believes that a common understanding of security concepts can help to make stakeholders aware of cybersecurity risks. DITTA also believes it is important for manufacturers and healthcare providers to adopt best practices and standards and to share those with other stakeholders.

2. Executive summary

Medical imaging devices are subject to risks that might harm their software, hardware or data security. Cybersecurity incidents may affect the safety of patients. This DITTA white paper is based on The Medical Imaging & Technology Alliance (MITA) who published in 2015 a white paper NEMA/MITA CSP 1-2016 Cybersecurity for Medical Imaging with fundamental security concepts in the medical imaging technology domain.

A critical component of cybersecurity in manufacturing is security-risk mitigation that is carried out while software is developed. User interfaces should not introduce complexity or barriers to devices' security capabilities. Manufacturers should define how they will continually monitor vulnerability to detect patches and updates. They should also allow healthcare providers to know the type and status of security software that is installed in devices.

Suppliers should test a device's vulnerability in its intended operational environment to determine what constraints operators must consider. Such penetration testing also identifies device vulnerabilities that the manufacturer should address.

Medical imaging (IT) manufacturers and hospital IT departments share responsibility for the technical infrastructure that must comply with best-in-class cybersecurity provisions and risk-assessment tools. A truly robust cybersecurity plan only can be achieved when there are clearly defined processes for cyber-prevention, when staff members are thoroughly trained in information and cybersecurity to enable them to follow those plans.

DITTA will remain a valuable global resource in the field of cybersecurity standards and regulations, in collaboration with professional organisations that represent medical imaging and IT professionals.

3. Device security

Medical device manufacturers should ensure that their products function as intended and meet safety and security goals. A device must guarantee the confidentiality of data, integrity of the device operation and availability of the device at any time, with respect to its intended environment and use—as specified by the manufacturer.

Manufacturers manage security risks by designing threat models based on use cases and the context of how a device is used. This can be achieved through creating visual aids to illustrate various ports, protocols and services used by the medical device. Data flow diagrams take into consideration information on how data is received, processed, stored or transmitted to and from the device.

Building security features into a device is a key concept for ensuring that the product not only meets regulators' standards in certain jurisdictions, but also for providing health care to patients in a secure way.

A critical component of cybersecurity in manufacturing is militating against security risk while software is being developed. User interfaces should not introduce complexity or barriers to a device's security capabilities. Instead, manufacturers should consider options for robust yet user-friendly, multi-factor authentication, including password fields allowing long strings (that can be remembered more easily, like user-generated passwords), access options for smart cards, biometric identification, and near field communication.

Manufacturers can ensure that they build security concepts into a product by embedding software assurance activities early in the software development life cycle (SDLC). Such concepts involve appropriate training for software developers, standardised coding practices and software code-testing as examples.

Manufacturers should also define how they plan to continually monitor device vulnerability in order to identify patches and updates that affect functionality or to repair vulnerabilities that might affect a particular device. Manufacturers also need to determine whether vulnerabilities affect the functionality and security of the device and, where appropriate, provide a validated patch. All software changes have to be validated to address cybersecurity before installation, to ensure that a device has not been compromised.

Manufacturers should also allow healthcare providers to know the type and status of security software installed in devices, including computers, routers and other at-risk components. They should also be aware of the status of security upgrades and particularly at-risk software. If devices communicate remotely using connections not covered by the healthcare provider’s firewall, they should have secure controls in place to access the network and use technology that does not compromise security.

Device implementations militate security risks using technical attack prevention (e.g. through device-hardening, firewalls and malware protection) and by technical response/recovery measures.

Manufacturers should also use so-called security white papers to document product-specific measures that an operator can take to minimise the exposure of the imaging

device embedded in the operational network.

4. External security

Equipment operators should take certain actions to safeguard their networked medical devices by deploying firewalls or other means to separate imaging devices and workplaces from external networks. Keeping third-party software at its current version protects products from known vulnerabilities.

Suppliers should close unused communication channels on their devices, such as ports or interfaces and disable auto-run features for external media. They should also test the vulnerability of a device in its intended operational environment to determine what constraints operators must consider in the field. Such penetration testing is also frequently used to identify whether a manufacturer must address any device vulnerabilities.

White-listing mechanisms can help to prevent malware code and can be integrated into a device before commissioning. This approach also protects against installing and running software not foreseen as part of the manufactured medical device, thus avoiding incompatibilities with authorised clinical applications.

Virus protection mechanisms are a good way to combat (known) threats, and suppliers should do basic assurance testing of imaging devices so that that virus definition and updated virus protection patterns do not affect the devices' clinical/operational functioning. Although virus protection can be interpreted as non-clinical functioning, updated patterns should be analysed and validated before they are released. This ensures that a device functions and performs properly post-update. In addition, anti-virus software should be configured to avoid 'false positives'; where essential clinical software is shown – wrongly - as infected with a virus.

5. Making communication more secure

Secure communication is essential when transmitting patients' health information between devices and recipients inside or outside an organisation. External communication should use up-to-date encryption standards such as HTTPS–TLS. Additional certificate-based authentication models can verify the identity of the user/system.

Digital Imaging and Communications in Medicine (DICOM), highly recognized at global level, is the standard for communicating and managing medical imaging information and is maintained by the DICOM Standards Committee. PS3.15 of the DICOM Standard specifies security and system management profiles that organisations can use as

guidelines for communicating with health data. Security and system management profiles are defined using externally developed standard protocols such as LDAP (Lightweight Directory Access Protocol), TLS (Transport Layer Security), and ISCL (Integrated Secure Communication Layer). Security protocols may use techniques such as public keys and smart cards. Data encryption can use various standardised data encryption schemes.

Increasingly, customers consider medical device manufacturers to be responsible as their devices interact with patient data. This means that manufacturers have to protect sensitive information and share responsibility for protection with the health care provider.

6. The responsible user

Most imaging modalities and all imaging informatics applications connect via the hospital intranet and/or a departmental intranet. Most of these, in turn, connect to the internet, albeit with security provisions such as a firewall. Within the healthcare field, medical imaging was one of the first areas to embrace the Internet of Things (IoT), the movement towards an increasing number of devices connected to the internet. Most, if not all, imaging technologies rely on digital technology, software and hardware connected to the internet; this can also make these systems vulnerable to cyberattacks.

Such attacks are potentially dangerous not only because patients' electronic health information may be disclosed but also because of the potential to compromise patient safety. Cyberattacks can disrupt how imaging modalities and imaging informatics applications function.

In cybersecurity, the maxim, "An ounce of prevention is worth a pound of cure" holds true. It is more important to take proactive, rather than reactive, measures. Preventing cybersecurity incidents will require cyber-awareness and training. Manufacturers' security White Papers help technology users to securely integrate a device or imaging IT into their network.

Medical imaging (IT) manufacturers and hospital IT departments share responsibility for the technical infrastructure that can comply with best-in-class cybersecurity provisions and risk-assessment tools. These include technologies such as physically segregated sub-networks for critical medical devices, VPNs, encryption, thin client technologies, high-availability IT infrastructure, data back-up mechanisms, firewalls and meeting the requirements numerous standards including ISO 80001, ISO 14971 and EN ISO 14971. However, a truly robust cybersecurity plan is only possible where cyber-prevention processes are clearly defined and followed by properly trained staff members.

Those responsible for handling the cybersecurity features of imaging modalities, image

and report distribution, or sharing and communicating (e.g., using encryption when creating CDs) should use the most up-to-date imaging IT processes. Manufacturers and hospital staff should discuss the following points with their IT departments:

- Auditing logs for imaging equipment and imaging informatics systems
- Changing how updating processes are managed
- Participating formally in organisation-wide cybersecurity planning
- Establishing operational communication processes with IT and cybersecurity resources of the Cybersecurity Systems Officer (CSO) and Cybersecurity Information Officer (CIO) (for example, to avoid penetration-testing incidents)
- Processing Incident Patient Information.

Manufacturers' field service representatives and training staff are also responsible for security measures. They should be aware of their customers' specific security requirements and abide by them. This includes obtaining prior permission from the appropriate customer IT security staff to insert flash drives or external computers into any component should that customer's protocols require it.

7. Resources needed for a security programme

Rather defining specific steps for establishing an effective security programme, we recommend that those responsible for cybersecurity measures refer to existing established best practices, resources, standards and tools. These can help users to maintain regulatory compliance and device security.

As an example, the security standard for supporting interpretation and implementation of ISO 27002[2] in health informatics is ISO 27799[3].

8. Suggested freely-available resources and public references

- HIMSS Risk Assessment Toolkit: This is designed to guide healthcare organisations through the security risk analysis and risk management process. Conducting a risk assessment will help to allocate budgets and other resources and mitigate actual risks faced by the organisation
- HIMSS Privacy & Security Toolkit: Additional privacy and security toolkits

[2] *ISO 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls*
[3] *ISO 27799:2016 Health informatics -- Information security management in health using ISO/IEC 27002*

- HIMSS list of Security Standards and Baselines
- 2016 HIMSS Cybersecurity Survey: HIMSS reports the survey of healthcare providers on their implementation of information security tools, motivations for using information security, etc,
- SANS 20 Critical Security Controls—focuses first on prioritising security functions that prevent the latest Advanced Targeted Threats, with a strong emphasis on what works; security controls where products, processes, architectures and services are in use that have demonstrated real world effectiveness
- Security Document Templates: A security management programme is built on administrative controls tailored to address risks faced by an organisation. Policies, standards, baselines, guidelines and procedures define how an organisation manages security. Additional administrative, physical and technical controls are implemented based on those policies. HIPAA requires specific documentation, and templates such as the SANS Information Security Policy Templates are available from organisations
- HIMSS/NEMA HN 1-2013 Manufacturer Disclosure Statement for Medical Device Security: This was developed by MITA and members of the HIMSS Medical Device Security Task Force in collaboration with multiple industry associations, government agencies and other stakeholders. This standard specifies a manufacturer's model-specific description of a device's ability to maintain or transmit electronically protected health information (ePHI) and the security features associated with the device. It also aids the healthcare provider's review and analysis of the large volume of security-related information supplied by manufacturers for medical devices installed on the provider's premises.

9. Resources that can be purchased

- RSAM: A suite of applications that can assist an organisation to meet various security goals
- Security Documentation[4]
- Security Awareness Training[5].

10. Conclusions

Cybersecurity in medical imaging is a shared responsibility between healthcare providers and manufacturers. Imaging staff must be aware of cybersecurity threats and current best practices. Security processes must be defined and implemented and the

[4] http://www.instantsecuritypolicy.com/index.html; http://www.complianceforge.com
[5] http://www.securingthehuman.org; http://www.knowbe4.com/products/kevin-mitnick-security-awareness-training/

proper technology must ultimately support zero-breach cybersecurity goals.

From a clinical IT perspective, some fundamental principles remain highly effective:

- **Awareness of responsible functions** among users is still the most effective form of prevention: Based on training and prevention processes, educated users are less likely to allow malicious access/content or to leak confidential information
- **Pro-active protection** in each domain means that any party involved should start with security processes that enable each organisation to identify, prevent and compensate any unintended or unauthorised use of products and IT systems
- **The principle of authenticity** ensures that activities and communication are performed with transparent and verifiable identification of all users involved. Messages must clearly identify senders and recipients and provide the means to verify these identities. This type of transparency does not only help recipients to detect and avoid unintended content, but also gives administrators the means to audit suspicious/malicious communication patterns
- During a device's whole lifecycle, manufacturers should **monitor and address its possible vulnerabilities**. Therefore, vulnerability information is quite important. Manufacturers and stakeholders such as operators, suppliers and users are recommended to exchange such information directly and promptly.

DITTA represents globally medical imaging device manufacturers and will continue to be a valuable resource in the field of cybersecurity standards and regulations, in collaboration with professional organisations representing medical imaging and IT professionals.

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 organisations. 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 DITTA website at http://www.globalditta.org/