Medical devices security – How to protect them

Theodor Adam, Florin Andrei, Larisa Gabudeanu, Victor Rotaru

Medical devices are fixed-function devices, designed to perform a specialized task. The lifecycle for medical devices may be as long as 10, or even 20 years. These are optimized devices to minimize processing cycles and memory usage, so they lack extra processing resources. In this context, the traditional information assurance approach Confidentiality-Integrity-Availability (the CIA triad) needs to be enriched with Safety-Reliability-Availability of the processes, devices and connected systems to strengthen the overall security posture. Nevertheless, we must include any safety functions and assess the consequences of malfunction to people, equipment and environment.

In our days, medical devices become a tightly integrated systems with complex data flows not only between devices, but also between devices and hospital IT systems. We should be aware that these devices are not only more vulnerable and difficult to protect, but also that the security compromise of any of these could result in patient harm or impact on care delivery – as we mentioned before, in addition to the traditional security concerns around data confidentiality, integrity, and availability. Considering the medical device lifecycle, the situation becomes even worst because we have to deal with different "generations" of devices and to build appropriate security measures around them in order to harden overall security.

According to NIST SP 1800-1, "All healthcare organizations need to fully understand the potential risk posed to their information systems, the bottom-line implications of those risks, and the lengths that attackers will go to exploit them… Assessing risks and making decisions about how to mitigate them should be continuous to account for the dynamic nature of business processes and technologies, the threat landscape, and the data itself…. We recommend that organizations implement a continuous risk management process as a starting point for adopting this or other approaches that will increase the security of the Electronic Health Records (EHR). It is important for management to perform regular periodic risk review, as determined by the needs of the business."

In the circumstances presented above, our security approach to protect our healthcare organization should have two directions:

- A strategic direction through a risk-based approach towards addressing threats.
- A tactical direction to harden the operational environment through Defense in Depth.

Threat modelling plays a vital part of the Security Development Lifecycle (SDL) process because it helps in identification of system vulnerabilities and threats and helps in establishing appropriate mitigation techniques. Threat modelling methodology involves optimization of Network/Application/Internet security through identifying objectives, threats, and defining countermeasures to mitigate the effects of the threat. Thus, threat modelling can be used in

medical devices to optimize mitigations through identification of threats and vulnerabilities to a specific device from an organization supply chain that can harm the patient.

The context of our work is depicted by the following security metamodel presented in Figure 1:

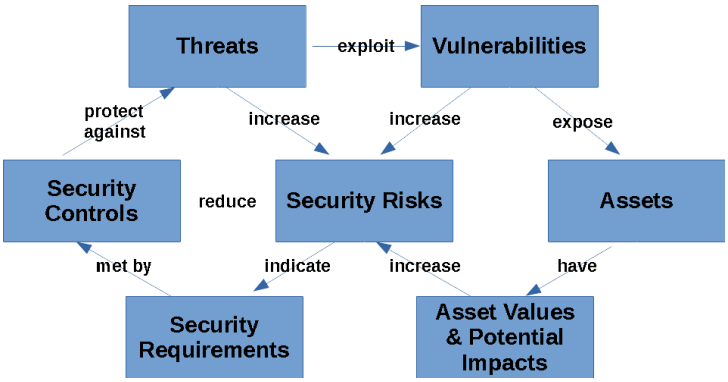


Figure 1. Security Risks Metamodel

We should be aware that the sources of the incidents are definitely worth an investigation in order to understand the most likely human based attacking vector that should be prevented or mitigated. According to any threat report, current employees are still the highest risk to cause new security incidents; however, but former employees and hackers are common threats as well. Addressing these threats with priority will improve the organization's risk posture.

1. Risk-based Approach Towards Addressing Threats

We need to keep permanently in our minds the fact that a compromised medical device may also serve as access point for the hospital networks with the purpose of stealing confidential data. Software incorporated in connected medical devices such as defibrillators, cardiac pacemakers, and network-connected X-ray machines is vulnerable to cybersecurity threats - some exploits could affect integrity of health data, availability of patient care, or even the manner in which the medical device operates.

Also, we need to be aware that there are different generations of technology we have to protect in a hospital, all of them doing great functional jobs, but also lack important security features and this might transform them in entry points for potential attackers.

The main objective is to design, develop and implement medical technical solutions that are secure throughout the whole life cycle without compromising patient safety. Therefore, we need to establish a framework to help us adjusting the hospital's risk posture. The framework we propose is presented in the Figure 2 and has the following main pillars:

a. Design Control – through a Cybersecurity Risk Assessment we identify the various information assets that could be affected by a cyber-attack (such as hardware, systems,

and patient data), and then we identify the various risks that could affect those assets. Either for a new technical solution or to redesign the security of the existing one, we need to define the requirements and applicable standards and then use them to design/redesign our technical solution, implement and test it. Before moving our project to the operational environment, we need to perform a penetration test in order to assure that our technical solution has no vulnerabilities based on current penetration testing best practices.

b. Operations Control – through Identity Access Management and Logging and Monitoring we keep track of the user activity. It is very important to keep our technical solution up to date (through Vulnerability and Patch Management). In case of incidents, the ability to respond and fix them is very important (through Incident Response process).

A particular care should be taken on Decommissioning. When we either need to clean-up the residual information from a project or we need to decommission the equipment, we need to ensure that the data is wiped properly using specialized, HIPAA (Health Insurance Portability and Accountability Act) certified, tools. The same applies for equipment disposal – in this case, considering the embedded risks, we would advise you to pass through the overall process (assess the risks, redesign the solution, implement it, test it, and the decommission the equipment, wipe the data and dispose it).

The selection of appropriate security controls at various life cycle stages of a medical device depends on:

i. Type of the medical device (e.g., device that contains software/firmware, device that contains programmable logic, software that is a medical device, mobile medical app, device that is considered part of an interoperable system, legacy device);
ii. Device classification;
iii. Intended use of the device;
iv. Operating characteristics of the device;
v. Sensitivity levels of contained data;

Therefore, appropriate Inventory Management is an important process you should have in place and a very useful source of information for the security team. This should be reflected also in the internal procurement procedures to ensure that this information is clearly obtained for each medical device purchased by the organization and is properly stored in an accessible form. Further, the specific EU legislation in place or pending entrance into force (such as Regulation (EU) 2017/745) for medical device production and maintenance has to be had in mind in terms of information and support received from medical device producers.

Regardless how well we will perform the risk management in our healthcare organization, there will always be residual risks we will need to address. The ongoing assessment of security threats, balanced against the existence and adequacy of security controls in our organization, is needed to ensure that security controls and countermeasures in place are commensurate with potential risks. Therefore, Cybersecurity Management Plan should be in place in order to provide guidance, effective planning, and proper risk management for the overall organization.

When we speak about cybersecurity risk assessment process, we refer to a process of estimation of the risks to the system posed by specific threats and vulnerabilities. This process consists of four tightly linked activities:

a. Analyze the capability of existing security controls to prevent an occurrence of the adverse event, detect an occurrence, and contain the impact of an occurrence.
b. Estimate the likelihood (high, medium, low) of an occurrence given the nature of the vulnerability, the capability of existing threats, and the strength of current controls.
c. Analyze the potential damage an occurrence would do to the system, its data, and the healthcare organization's goals. Rate the potential impact as high, medium, or low.
d. Derive the risk rating from the combination of likelihood and impact.

Another important aspect in the security management of our healthcare organization is the communication with the employees. All the findings, threats, recommendations, guidance you consider useful should be assembled in a security whitepaper and made available to all employees. This is not a replacement for awareness training.

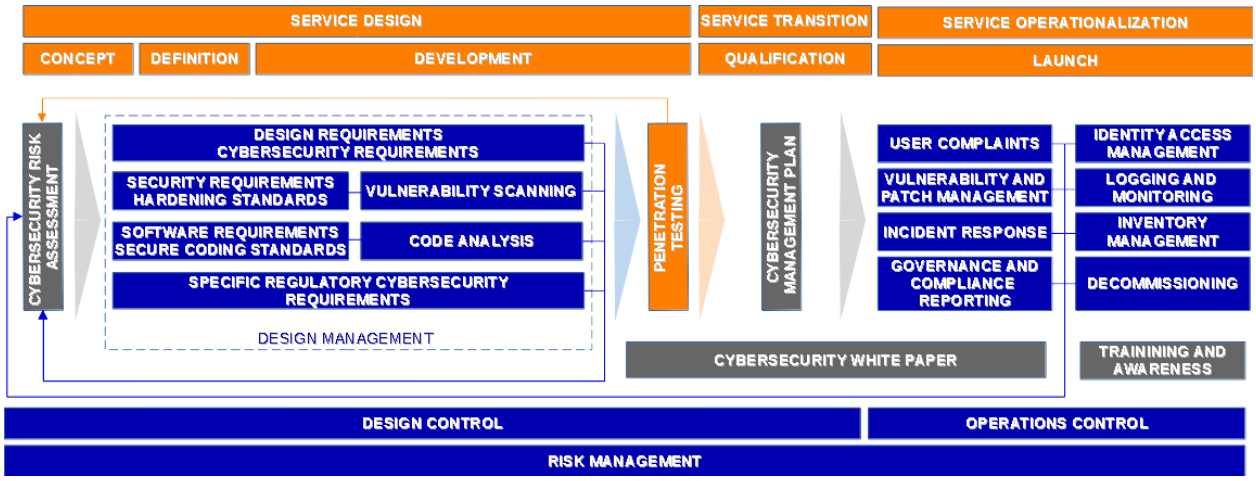


Figure 2. Risk-based Approach towards Addressing Threats

2. Hardening the Operational Environment through Defense in Depth

One of the most effective ways to ensure CIA is to take a defense-in-depth or layered approach when addressing privacy and security issues. A tiered approach avoids a single point of failure and supports layered controls in case one of the controls is compromised or does not operate as intended. Considering the heterogeneous environment we have to protect, Defense in Depth is the information assurance concept we should employ in order to build appropriate layered security mechanisms able to keep threat actors as far as possible from our critical assets.

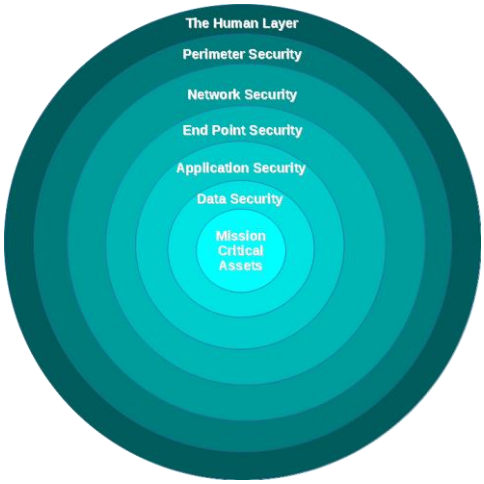


Figure 3. Layered Security to Protect Mission Critical Assets

Human Layer – Humans are considered the weakest link in any cybersecurity posture. Only through user training and awareness we can establish a security conscious culture within organization and deliver security knowledge to employees.

How can the risk be managed?

a. *Produce a user security policy*: Develop a user security policy, as part of the organization's security policy with the aim to have adequate authentication and authorization mechanisms in place, and by considering the need to know and data minimization principles. Security procedures for all systems should be produced with consideration to different roles and processes.

b. *Establish a staff induction process*: New users (including contractors and third party users) should be made aware of their personal responsibility to comply with the organization's security policies as part of the induction process, with practical examples tailored to their role in the organization.

c. *Maintain user awareness of the security risks faced by the organization*: All users should receive regular refresher training on the security risks to the organization together with specific messages on particular threats at a given time (e.g. a new ransom ware targeting hospitals) through a delivery means appropriate for such important messages.

d. *Monitor the effectiveness of security training:* Establish mechanisms to test the effectiveness and value of the security training provided to all users. This will allow training improvements and the opportunity to clarify any possible misunderstandings.

e. *Promote an incident reporting culture*: The organization should enable a security culture that empowers staff to voice their concerns about poor security practices and security incidents to senior managers, either anonymously or not. This is also in line with upcoming legislation on whistleblowers.

f. *Establish a formal disciplinary process*: All staff should be made aware that any abuse of the organization's security policies will result in disciplinary action being taken against them. All sanctions detailed in policy should be enforceable at a practical level.

g. *Support the formal assessment of security skills*: Staff in security roles should be encouraged to develop and formally validate their security skills through enrolment on a recognized certification scheme. The same approach should be taken for IT-related staff in order to ensure proper implementation of security requirements.

Perimeter Security – the point in which we have control of our network, technology, and data. It is a defense system around our network designed to stop malicious attacks from entering.

How can the risk be managed?

There are many technologies available to you to help secure your network perimeter:

- Firewalls.
- Intrusion Prevention System (IPS).
- Intrusion Detection System (IDS).
- Unified Threat Management (UTM).
- Messaging Security (Antivirus, Antimalware).
- Data Loss Prevention (DLP).
- Secure De-Militarized Zone (DMZ).
- Virtual Private Network (VPN) solution for remote users' access.

Network Security - the techniques and tools to protect your network data from malicious threats and save your organization from destructive losses. Your techniques require you to know how to protect, detect, respond, and predict a broad range of attacks.

How can the risk be managed?

Key techniques and tools include:

- Access control: To improve your network security by restricting user access and resources to just the sections of the network that clearly relate to. Role based access control upon the level of need to know of each defined role. Proper management of new arrivals and departures/changes in user role are an essential part of proper implementation of access control, with a specific internal process generally being designed in this respect.
- Antimalware and antivirus software: To detect malicious programs and stop them from spreading.
- Anomaly detection: Implement network anomaly detection engines (ADE) to evaluate your network, recognize anomalies and respond to them.
- Application security: Implement additional security measures for critical applications to your network security.

- Data Loss Prevention (DLP): Prevent personnel and other users from abusing and potentially compromising valuable data.
- Endpoint security: Additional layer of defense between organizational networks and remote devices.
- Intrusion prevention systems: IPD/IDS protect from known attack vectors so threats can be recognized easier.
- Network segmentation: Give appropriate access to the appropriate traffic while controlling the traffic from other users or sources.
- Web security: Prevent web-based threats such as malicious scripts, or adware programs to leverage browsers as access points to penetrate your network.
- Two-factor authentication: Adds an additional layer of security to the authentication process by making it harder for attackers to gain access.
- Virtual Private Network (VPN): An encrypted connection over the Internet from a device to a network to ensure that sensitive data is safely transmitted.
- Data at rest encryption: To prevent unauthorized access to your data.
- Encrypted backups: An extra security measure to protect your data.

End-Point Security - refers to securing endpoints, or end-user devices like desktops, laptops, and mobile devices. It includes data security, network security, advanced threat prevention, forensics, endpoint detection and response (EDR), and remote access VPN solutions.

How can the risk be managed?

There are many technologies available to you to help secure your end points:
- Content Security: Anti-virus & anti-malware software.
- Patch Management.
- DLP.
- Endpoint Detection and Response (EDR): EDR “watches” the endpoint, looking for security problems or anomalous behavior that might indicate an attack or compromise.
- Virtual Private Network (VPN).
- Local/host firewall.
- End Point security policy enforcement.

Application Security - measures taken to improve the security of an application often by finding, fixing and preventing security vulnerabilities.

How can the risk be managed?

The following technologies and techniques are available to help you secure your applications:

- Static Application Security Testing (SAST): scans the application source files, accurately identifies the root cause and helps remediate the underlying security flaws.
- Dynamic Application Security Testing (DAST): simulates controlled attacks on a running application or service to identify exploitable vulnerabilities in a running environment.
- Server Patch Management.
- Web Application Firewall (WAF): helps protect your web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources. A WAF is deployed to protect a specific web application or set of web applications.

Data Security - the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. It refers to data security controls required to protect the storage and transfer of data.

How can the risk be managed?

The following technologies and techniques are available to help you secure your data:

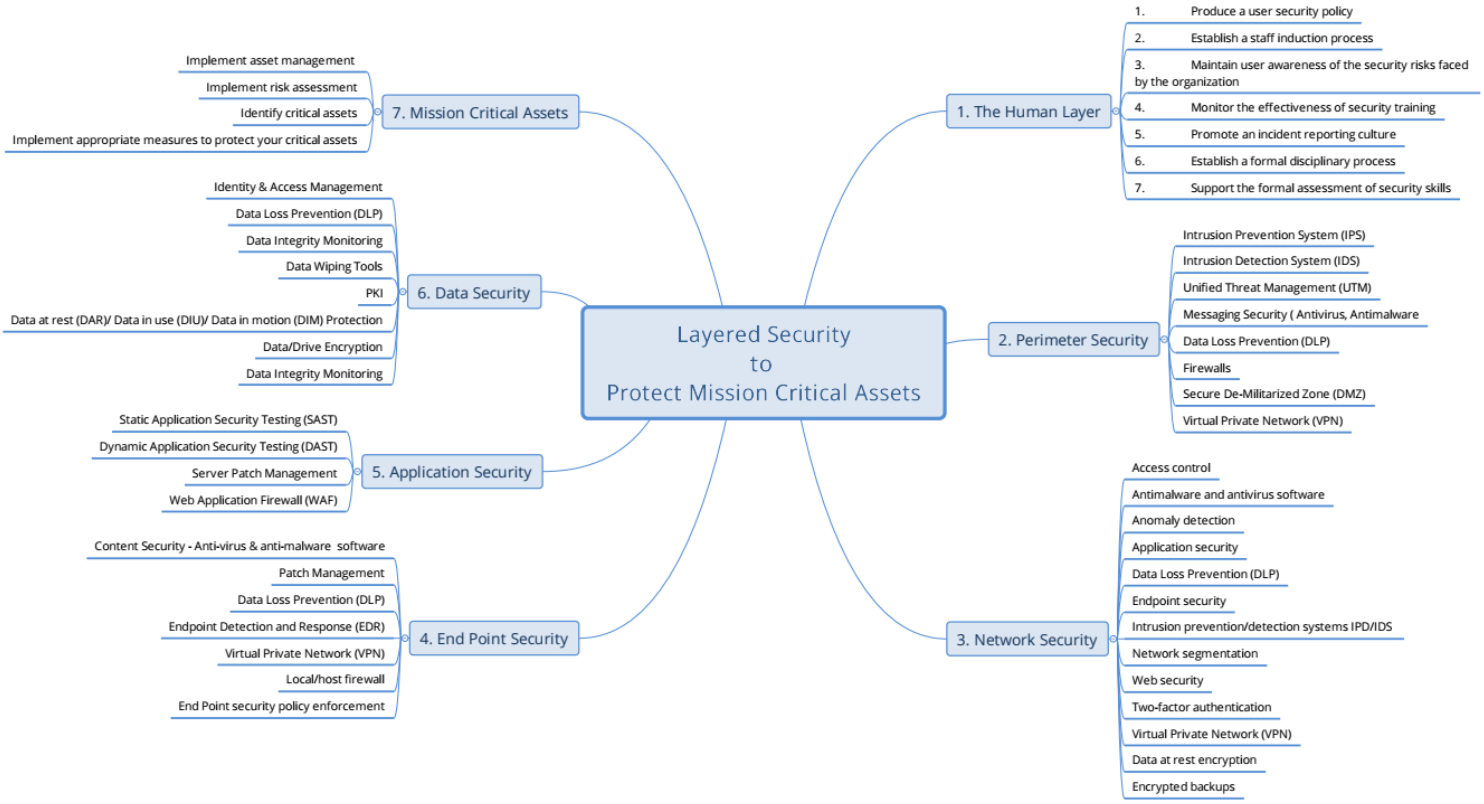
- Identity & Access Management.
- DLP.
- Data Integrity Monitoring.
- Data Wiping Tools.
- PKI.
- Data at rest (DAR)/ Data in use (DIU)/ Data in motion (DIM) Protection.
- Data/Drive Encryption.
- Data Integrity Monitoring.

Mission Critical Assets – devices, applications, databases and data that are crucial for your organization – without them your organization cannot operate. The following links https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis/at_download/fullReport and https://www.enisa.europa.eu/publications/security-and-resilience-in-ehealth-infrastructures-and-services/at_download/fullReport describe ENISA methodology and recommendations for eHealth Critical Asset Protection.

How can the risk be managed?

- The following steps should be fulfilled in order to identify and protect your critical assets:
- Implement asset management
- Implement risk assessment
- Identify critical assets
- Implement appropriate measures to protect your critical assets

The following mindmap depicts the Layered Security to Protect Mission Critical Assets presented above.



3. Conclusions

Both perspectives presented in this article, Design Control and Operations Control (through Defense in Depth) have something in common – the need of risk assessment before taking any action. Considering that we deal with limited resources, it underlines even stronger that risk assessment, vulnerability analysis and incident response are the minimum required three main pillars you should have in place in order to protect effectively your organization.