



Preparing for EU MDR/IVDR Medical Device Cybersecurity

CyberActa, Inc.

Webinar

April 14, 2021 10:00 AM EST



Agenda



Speaker information & background



Brief Introduction to Cybersecurity



Medical Device Cybersecurity expectations under EU MDR/IVDR



Establishing your own Medical Device Cybersecurity Program



Guiding Questions



Q&A

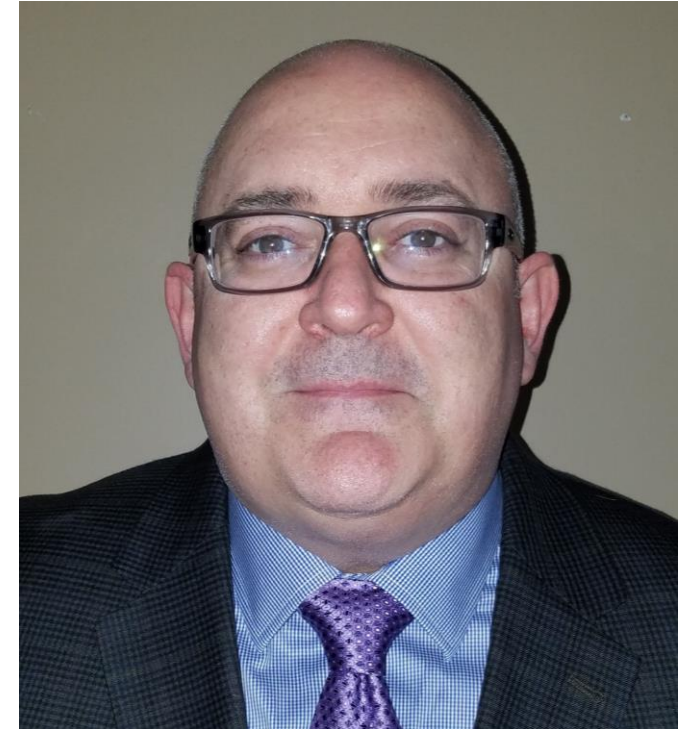


Speaker Information – John Giantsidis

John Giantsidis advises clients on matters spanning the product life cycle, from product development and clinical trials, through FDA, EMA, PMDA, and TGA premarket review processes, to post-market compliance, GxP practices, software validation, and Quality System requirements. Whether traditional medicinal products and devices, rapidly evolving medical and health technology products, such as a SaMD or digital diagnostic tools, he has extensive knowledge of the governing laws and regulations and broad-based practical experience with their application in advising clients to achieve competitive advantage by guiding on significant events that could adversely affect product quality, submission approval, compliance status, or pose a significant business risk.

John is a member of the Florida Bar's Committee on Technology and a Cyber Aux with the U.S. Marine Corps. He holds a Bachelor of Science degree from Clark University, a Juris Doctor from the University of New Hampshire School of Law, and a Master of Engineering in Cybersecurity Policy and Compliance from The George Washington University.

He frequently writes and speaks on a broad range of current issues facing the MedTech and life sciences industries such as building privacy and cybersecurity in medical devices, the evolving regulatory landscape in this rapid pace of technology-driven change, and addressing the challenges of product development, testing, generation of evidence, proof of value, implementation and adoption of novel medical and health technologies.



John.Giantsidis@cyberacta.com



Enabling Security & Privacy in Digital Health

Strategic & tactical medical device cybersecurity, risk management, privacy, SaMD/SiMD regulatory compliance consulting.

Medical Device
Cybersecurity
Management

SaMD/SiMD
Development &
Commercialization

Privacy & Data
Governance

Software
Validation & Data
Integrity

Education &
Training

Design Controls &
Risk Management

Regulatory
Submissions &
Compliance



What Is Cybersecurity, and Why should you Care?

HINT → YOUR REGULATORS AND CUSTOMERS DO!



Cybersecurity

- Consider cybersecurity as the ongoing application of those best practices intended to ensure and preserve confidentiality, integrity, and availability of digital information as well as the safety of people and environments.
- The pillars of cybersecurity used to be a triad: confidentiality, integrity, and availability. However, in medical device cybersecurity, safety is the newest member of the roster and introduced to address everyday-life threats posed by the Internet of Medical Things (IoMT).
 - **Confidentiality** – The means of protecting any asset from being accessed by unauthorized parties
 - **Integrity** – The consistency, accuracy and trustworthiness of your process or output over its entire lifecycle
 - **Availability** – The set of practices and tools designed to ensure timely access to data.
 - **Safety** – The activities and consideration for any cybersecurity incidents that could result in injuries, and even loss of life.

Cybersecurity is a disciplined process



Complex

Cannot be managed informally.



Formal Processes

Planned series of actions in security management
Annual planning.
Processes for planning and developing individual countermeasures.



A Continuous Process

You will fail if you let up



Answer these 3 questions



What needs to be protected?



How much protection is needed?



For how long is the protection needed?



Attacks

Confidentiality

- Interception
- Disclosure

Integrity

- Interruption
- Modification
- Fabrication
- Corruption

Availability

- Interruption
- Modification
- Fabrication
- Removal
- Destruction



Cybersecurity Risk Management

Identify, assess and reduce risk to an acceptable level.

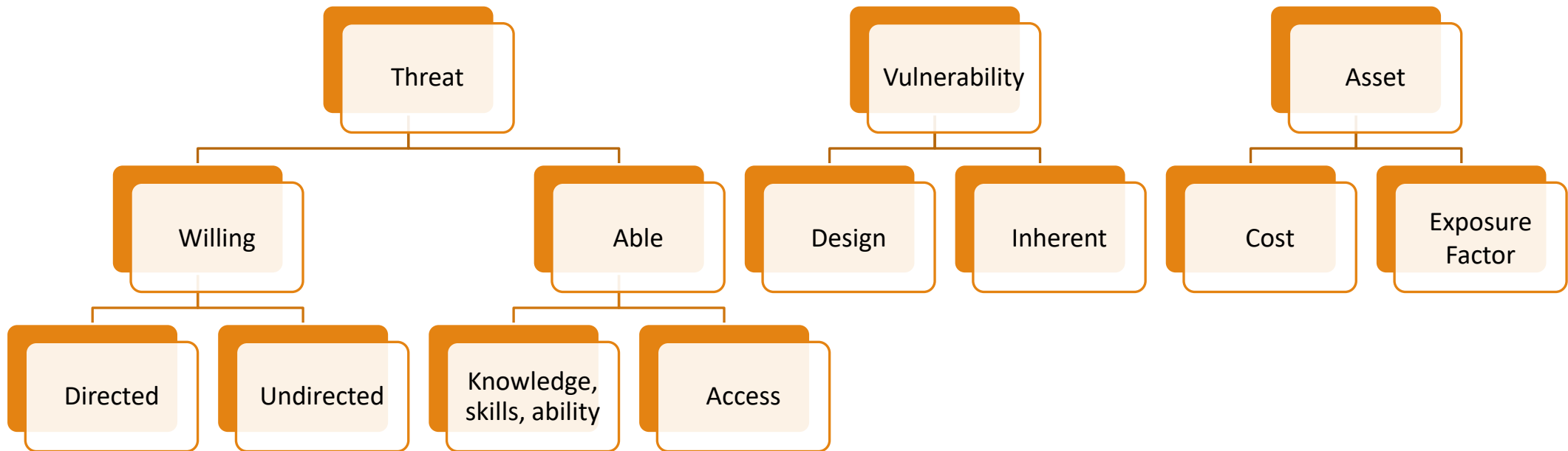
Risks can be identified & reduced, but never eliminated.

Even if it were possible to eliminate all risk, the cost of achieving that total risk avoidance would have to be compared against the cost of the possible losses resulting from having accepted rather than having eliminating risk.

The results of such an analysis could include pragmatic decisions as to whether achieving risk avoidance at such cost was reasonable.



The "Simple" Risk Model





Some helpful terms

Vulnerability – A weakness in an asset that can be exploited by a threat to cause harm

Threat – Any circumstance or event with the potential to cause harm to an asset

Asset – Anything that needs to be protected

Countermeasure – A safeguard used to mitigate the potential losses from an identified threat (safeguard is a control executed to reduce the risk that is associated with the specific threat)

Cyber countermeasure – An action, process, technology, device, or system that serves to detect, prevent, or mitigate the effects of a cyber attack against a victim, computer, server, network, or associated device.

Risk – Probability of a threat agent exploiting a vulnerability

Compromise – A successful attack; aka incident; aka breach

Medical Device Cybersecurity

EU MDR/IVDR



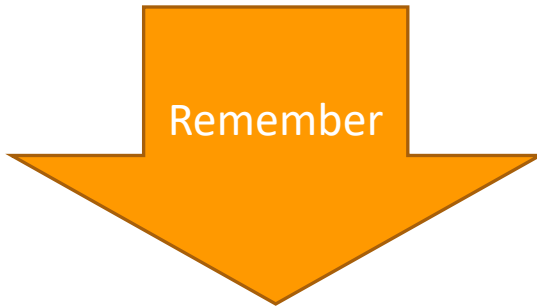
Cybersecurity Legal Basis under EU MDR

- The General requirements cover cybersecurity in principle (**Annex I, No.1**)
- Principle of integrated security: risk control measures mandatory in order of safe design and production, appropriate safeguards with regard to risks that cannot be excluded, Security information and, if necessary, training (**Annex I, No.4**)
- Risk management, among other things, for the identification and analysis of known and foreseeable hazards is mandatory (**Annex I, No. 3b**)
- Risk minimization associated with the possible negative interaction between software and the IT environment in which it is used and interacting with it (**Annex I, 14.2**)
- Appropriate precautions shall be taken to eliminate or reduce any risks or performance impairments arising from #defects. (**Annex I, No. 17.1**) and finally
- Software shall be developed and manufactured according to the state of the art, with principles of a software lifecycle, risk management, #informationsecurity, verification, and validation. (**Annex I, 17.2**)



MDCG 2019-16 Guidance

- Endorsed by Medical Device Coordination Group (MDCG) established by Article 103 of Regulation (EU) 2017/745; we are waiting for the EU IVDR Guidance
- It is simply a guidance or roadmap that manufacturers can use to develop and manufacture their products in accordance with the state of the art, considering:
 - Risk Management
 - Information Security



Cybersecurity is part of the new essential safety requirements for all medical devices that incorporate electronic programmable systems (SiMD) and software that are medical devices in themselves (SaMD)



Warning!

MDCG is outdated.

Aging "Defense in Depth" cybersecurity no longer works well against today's targeted, zero-day cyberattacks

INCIDENTS BECOME MORE SOPHISTICATED AND PERSISTENT; MEDICAL DEVICE MANUFACTURERS NEED TO MOVE AN EFFECTIVE CYBER RESILIENCE PROGRAM THAT INCLUDES A PROGRAMMATIC APPROACH TO WITHSTAND DISRUPTIVE CYBER INCIDENTS.

A SIMPLE WAY TO LOOK AT AN EFFECTIVE CYBER RESILIENCE MODEL CAN BE TO KEEP IN MIND THE THREE P'S : PREDICT, PRIORITIZE AND PRACTICE.

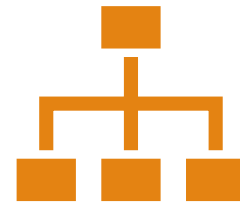


How to start your Medical Device Cybersecurity Program?

HERE IS A 7 STEP PROGRAM TO CONSIDER



Step 1 – Prioritize and Scope



The organization identifies its business/mission objectives and high-level organizational priorities.



With this information, the organization makes strategic decisions regarding medical device cybersecurity implementations and determines the scope of systems and devices that support the selected business line or process.



Step 2 – Position

Once the scope of the medical device cybersecurity program has been determined for the business line or product, the organization identifies related systems and assets, regulatory requirements, and overall risk approach.

The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.



Step 3 – Create a Current Profile

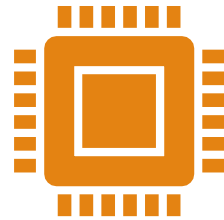
THE ORGANIZATION DEVELOPS A CURRENT MEDICAL DEVICE CYBERSECURITY PROFILE.



Step 4 – Conduct a Risk Assessment



This assessment should be guided by the organization's overall product risk management process or previous risk assessment activities.




The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on medical device.



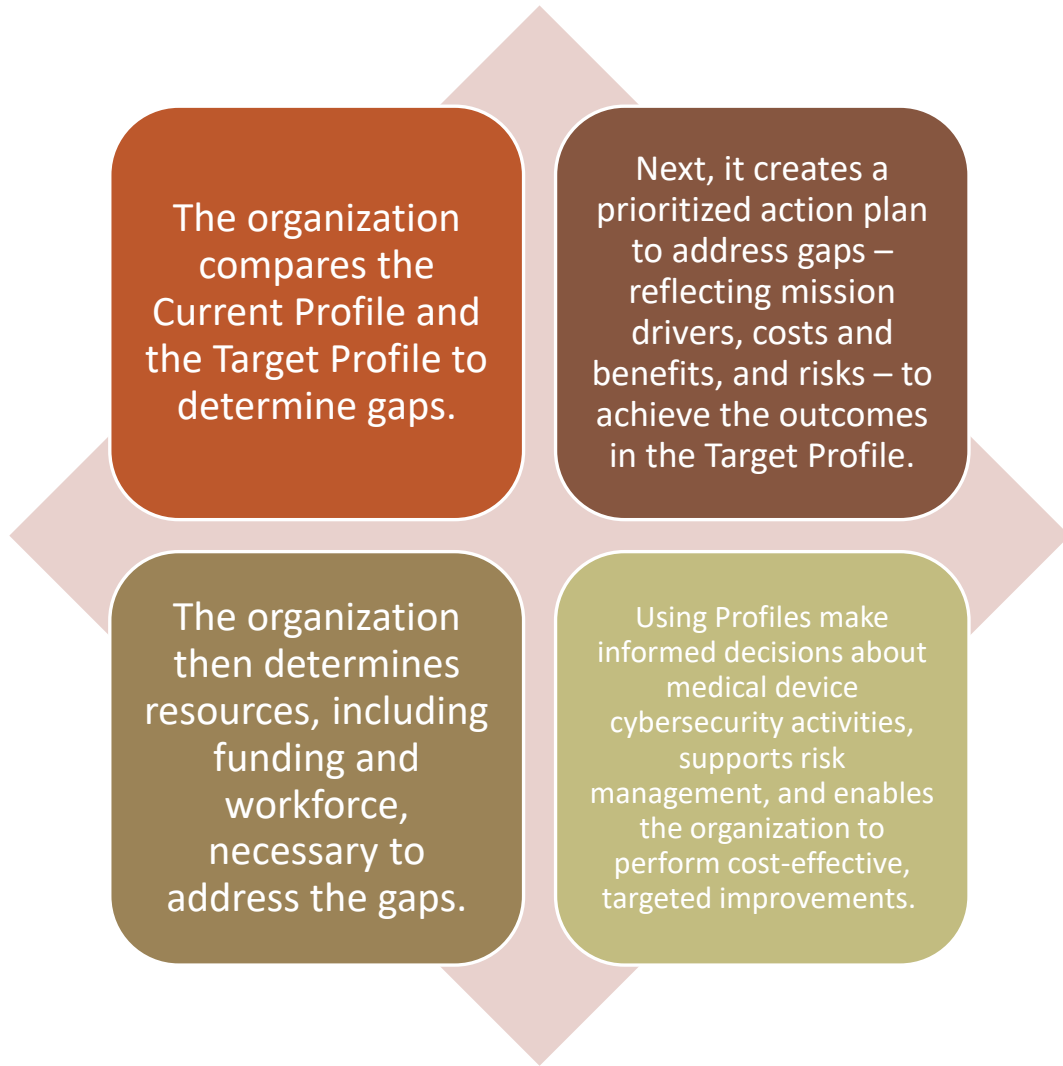
It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5 – Create a Target Profile

The organization creates a Medical Device Cybersecurity Target Profile that focuses on the assessment describing the organization's desired cybersecurity outcomes.



It is important to understand that a Target Profile should be created for each medical device or family of medical devices.



Step 6 – Determine, Analyze & Prioritize Gaps




Step 7 – Implement Action Plan

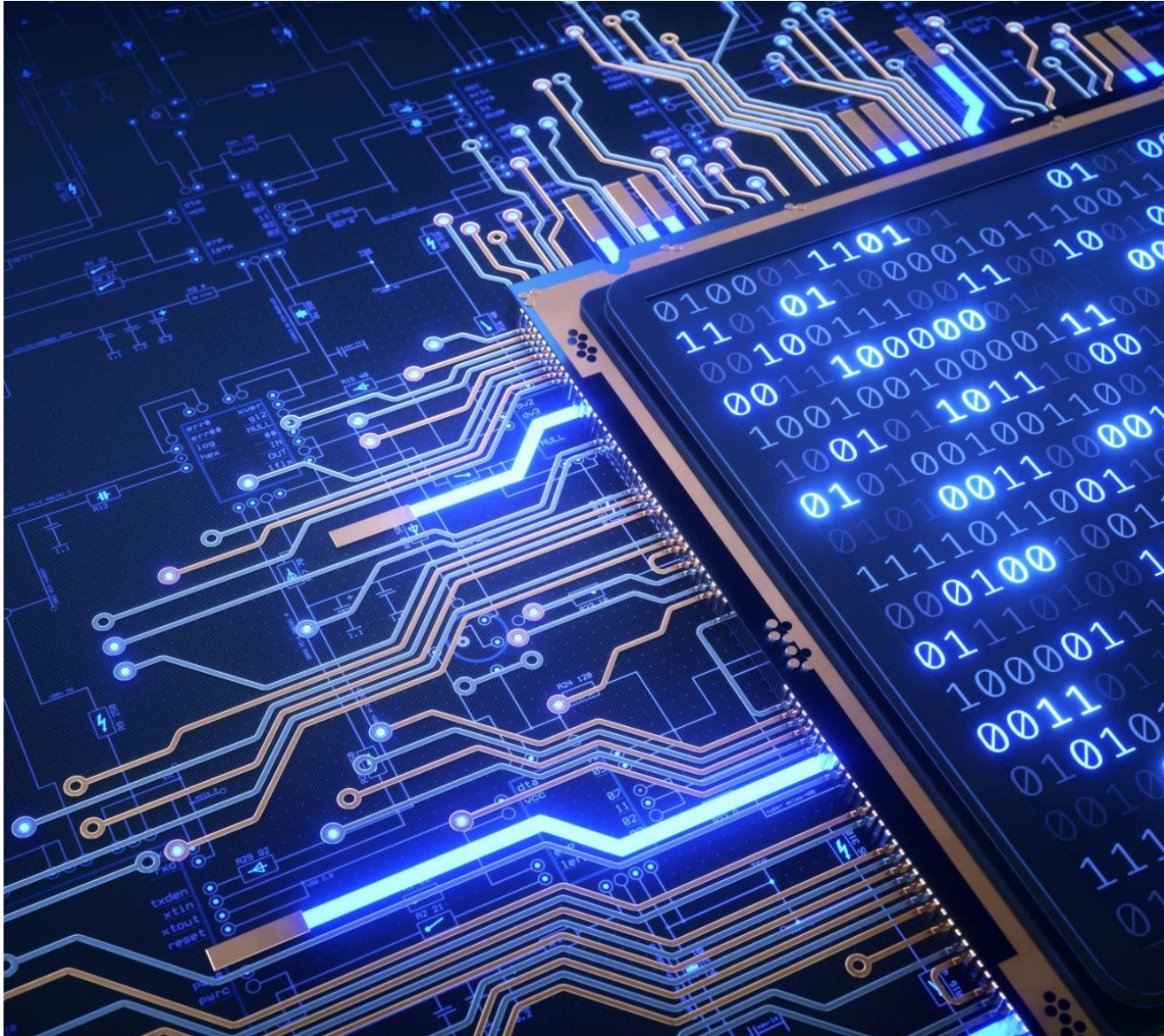
The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile.




Guiding Questions



Has
cybersecurity
been considered
in the design of
your medical
device?



Does the intended use of your device expose it to risks associated with cybersecurity (will your device connect to networks, will it transmit data)?



Can the performance, reliability, and repeatability of the device be impacted by cyber vulnerabilities?

The hardest to
answer

Is there a risk that a cybersecurity vulnerability may lead to your medical device compromising the health and safety of the user (patient or operator)?

Is that risk acceptable?



Questions?

THANK YOU FOR YOUR ATTENTION



Remember

- Operating systems are part of the medical device and are therefore also the subject of the conformity assessment procedure

- Cybersecurity is the subject of the vigilance system
- Security patches to prevent death or serious deterioration of a person's health due to IT vulnerabilities are reportable corrective measures



What's next?

- Performance of **threat modeling** in the device life cycle to drive initial identification of threats and associated compensating design controls
- Identification and detection of **security vulnerabilities** through the performance of security risk assessments for devices during development (conduct security risk assessment for devices in the market that did not undergo assessment during development)
- Performance of **security testing** (i.e., application, interface, hardware, firmware) for devices in development (also conduct security testing for devices in the market that did not undergo a testing during development)
- Assessment of the specific product being procured from third party product/component vendors at the product level for technical cybersecurity vulnerabilities leveraging the manufacturer's product **security design requirements** and security risk assessment and testing methodologies
- **Monitoring** of components (hardware and software) for known security vulnerabilities
- Storage and maintenance of the results of security risk analysis to facilitate monitoring and alignment with **design changes** and evolutions in industry leading practices