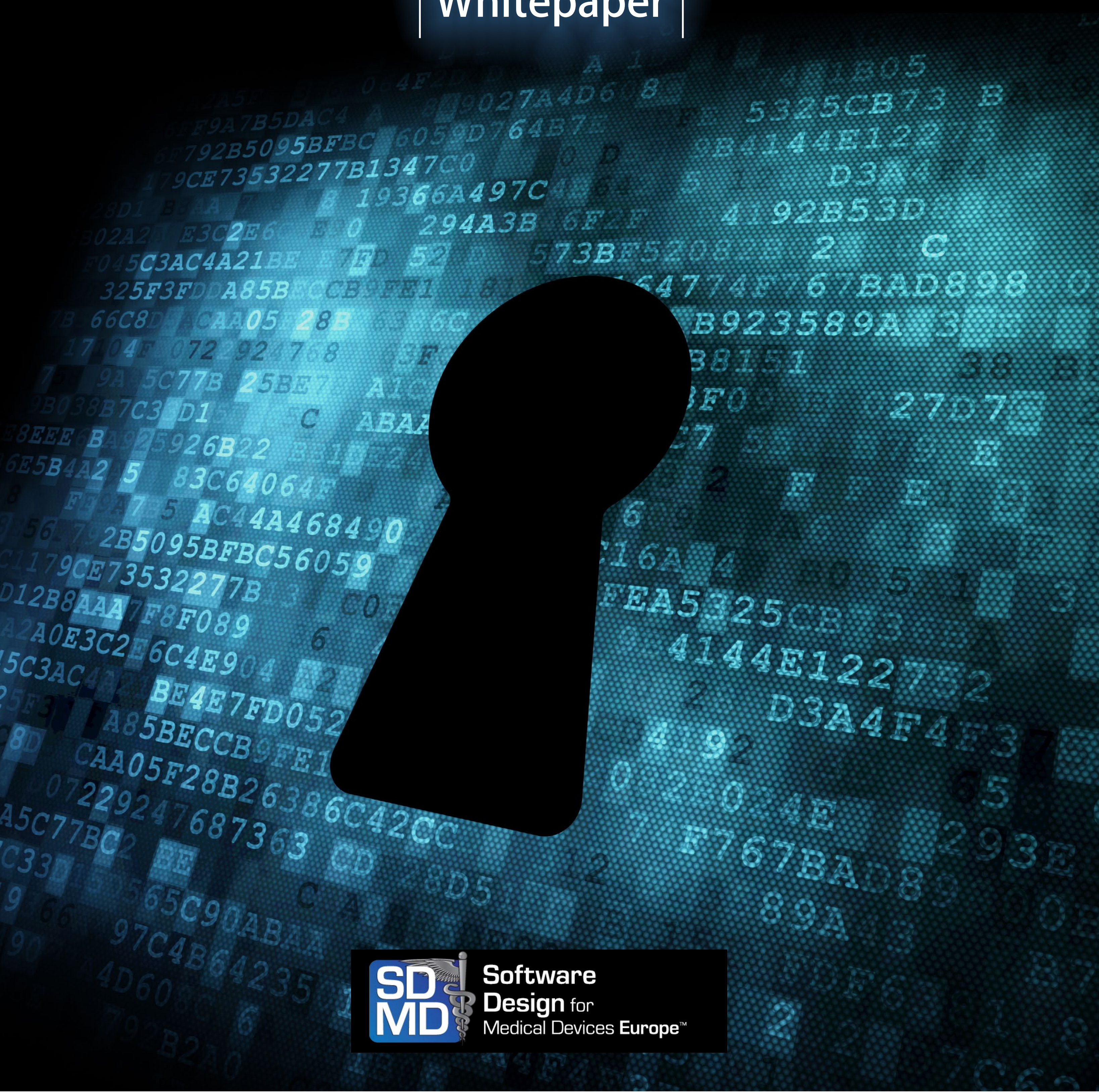
Software for Medical Devices Cyber Security

What You Need To Know

| Whitepaper |



SDMD Software Design for Medical Devices Europe™

The world of healthcare has greatly benefitted from enhanced connectivity as a by-product of the digital age. However, this benefit has contributed to exposing medical devices and their softwares to cyber attacks. Malicious digital interferences can be significantly detrimental to patient safety. Cyber security initiatives require attention from various areas for example - systemic and technical perspectives.[2] Security researchers have been uncovering hazardous flaws recently with medical devices to help with awareness on the various intervention methods which may be used.[1]

Surprisingly, it is felt that spending on medical devices is still not high enough. ABi Research forecasts that healthcare provider spending on cyber security for healthcare will reach $5.5 billion in 2016. However, only $0.3 billion is due to be channelled for medical device security.[5] Growing awareness of this new hostile arena will push spending in this area forward. The intelligence firm states that millions of connected medical devices bring fresh threat vectors into the healthcare IT landscape. These could have damaging impacts on effective care delivery and patient safety if left unmonitored.

Recent guidance published by the FDA has reinforced the responsibilities expected of medical device software manufacturers in regards to the cyber security of their products. The guidance covers disclosing vulnerabilities and implementing remediation programs to monitor and fix any security issues. Proactive planning and risk controls stand as key requirements for new products and those on the market currently.1

Ahead of the 2017 Software for Medical Devices conference, Pharma IQ brings you this whitepaper looking at what you need to know in regards to software cyber security to medical devices.

Contents

Software Design for Medical Devices

Cyber Attack Fact File

How Cyber Attacks on Med Devices happen:

The direction of information is now more sophisticated with medical devices. They connect with remote devices and networks and so can no longer be deemed as standalone devices. Implant devices can be altered remotely, pacemakers, insulin pumps are some examples of these. This openness creates vulnerabilities. Security measures must account for the flow of communication, as attacks can occur through having physical contact with the device or remotely. 2 Digital attacks can even be unintentional for example an infection obtained via a corrupted USB stick inserted by an administrator.[2]

Attacker Motives: These can range from financial rewards through organised crime, to make political statements or even state sponsored targeting.

Detriment caused: Security weaknesses in medical devices expose the data held and in some instances the control of the device itself. If the configuration is not adequate or data has been corrupted, patient safety is at risk of attackers influencing clinical decisions or even operating the device. Attacks can be coordinated to block access to information – disabling critical alerts or clinical information being transmitted via malware and other hacking softwares. Aside from patient safety risks, other areas of potential harm include non-compliance, litigations and financial penalties.

Modes: Web servers can be an infiltration point when they provide an interface to control devices. Others targets for attack include database servers. Software can be compromised using these channels with the use of viruses, trojans and malicious software. According to Patricia AH Williams and Andrew J Woodward in Cybersecurity vulnerabilities in medical devices there are tools online which have the ability to assess web interfaces and pinpoint software vulnerabilities that should be targeted. Multiple live medical devices are known to have fallen victim to cyber attacks because their software has gone through inadequate vulnerability testing.

Vulnerabilities: Security holes can be created from backdated operating systems and/software – also incompatibilities between systems. Inadequate software updates and patches can be key culprits. The finite power attached to medical devices complicates encryption processes can cause med devices to lag and drain battery life.

Enhancing cyber security

Software Design for Medical Devices

Cyber Security Standards

Standards

- FDA Premarket Cybersecurity Guidance — View
- FDA Postmarket Cybersecurity Guidance DRAFT: — View
- IEC 80001-2-2: — View
- IEC 80001-2-8 — View
- IEEE Building Code for Medical Device Software Security Guidelines — View

> “Manufacturers will need to continuously monitor the security of their devices.“

Compliance considerations

The FDA is leading the way in regards to cybersecurity for medical devices. Anita Finnegan, CEO of Nova Leah Ltd provides an overview of the timeline so far in regards to FDA guidance on cyber security for medical devices:

“The FDA issued the first security-specific Safety Communications starting back in 2013/2014. Later in 2014 FDA published the first Premarket Cybersecurity Guidance document. This document sets out recommendations and requirements for medical device manufacturers to implement cybersecurity processes into lifecycle development processes. Until this, manufacturers were concerned only with demonstrating medical devices to be safe and effective, but now, they need to balance that with a third perspective and demonstrating the security assurance of medical devices.

Earlier this year the FDA progressed further and published a second cybersecurity guidance. This was the Postmarket Cybersecurity Guidance [draft] document. For a medical device manufacturer, following this guidance requires significantly more effort than the Premarket Cybersecurity Guidance. The document sets out recommendations for manufacturers to implement cybersecurity processes during the entire operational lifetime of a device”.

TIP: “A key consideration for improving security assurance of devices is to start early in the lifecycle process. Build cybersecurity in to the development lifecycle from concept stage and maintain a level of practise through to product retirement. A noted failure from other critical industries is when cybersecurity is considered at the end of the development lifecycle prior to product release. Discovery of security issues at this stage could be very costly to a developer. Cybersecurity should be a consideration across the development team, across the entire lifecycle.”

Software Design for Medical Devices

Cyber Defence Strategies

from the first stages of development

In industry whitepaper, The Open Web Application Security Project 7 notes that the most important measure to deploy in any software project is to verify for security early and often. Security testing can often be conducted outside of development testing loops, using a scan- fix approach in later stages. The apt method is in fact to ensure that security testing is within the developers' software engineering practise by using manual or automated tests. Agile approaches like test driven development are useful for placing responsibilities on developers to test their own work using swift feedback cycles.

In some cases it is a learning curve for medical device manufacturers to incorporate cyber security considerations. In these scenarios it is vital to understand the implications of certain processes in the development that could impact the safety or the security of a device.

Standards and best practice models will provide guidance in determining the best features to add to devices and how the should be deployed. They can also provide information on the vulnerabilities to safeguard with controls and capabilities. In writer requirements cover considerations for security, this will be beneficial to manufacturers implementing protections more seamlessly into development lifecycles.

Massimiliano Nobile Project Manager at Flex said that in regards to addressing software risk analysis with some cybersecurity is possible to start in advance to the availability of the draft software architecture. For example, if IOS is the confirmed platform, even though there is not a line of code for this project yet, the cybersecurity assessment can be started related to the services that will be used.

Training - ensure developers are aware of the considerations outlined in standards and are implementing them. This way cyber security programmes can be implemented into an organisation's development processes and also to the wider ecosystem. Also, consider the impact of QA and that of senior management on that system.

Be aware of customer preferences: Customers will have set ideas in terms of their environment and the intended use of a system, it's important to hold an understanding of what this healthcare provider would want to see. Anita Finnegan said that work being conducted in regards to the IEC 80001 dialogue framework has been vital to allow the relevant healthcare stakeholders to communicate about cyber security issues of their devices

Cost efficiency

Cost efficiency can be obtained by implementing cyber security practices on a gradual basis. Anita Finnegan clarifies that manufacturers could decide to utilise process assessment models whereby they can implement baseline cyber security requirements into a product and build from there. She adds that it is possible to overextend cyber security initiatives. Therefore, it's crucial to strike the correct balance through understanding the requirements and potential risks, and the most effective necessary measures to be implemented.

In FDA standards engagement with ISAOs is covered. Anita Finnegan explains that these bodies exist to enable the safe sharing of information between stakeholders: software developers, manufacturers, regulators and healthcare providers. Participation in this exchange will have cost benefits as the community acts as a good primary source of intelligence on the attack and defence methods in the market.

Process efficiency

The use of Agile methods for medical device software cybersecurity development is referenced in the TIR45 FDA guidance. Massimiliano Nobile notes that this approach gives manufacturers more project visibility and control to correct trajectory when needed. A high level of testing will be needed to verify design control during Agile development.

High levels of quality can be obtained through Agile processes if manufactures keep in parallel with feature development, design control activity, risk management and testability design. Design for testability can be a vital stage. Massimiliano Nobile explains that in finalising a project some surprises may be encountered because a product's feature delivery and system acceptance were followed, but then the novel layers of the product have lost testability characteristics.

At the end of development when the design is mature focus on big white box testing. It would not be cost efficient to undergo deep white box testing while features are still changing.

Continuous Monitoring: A sentinel monitoring of the technologies used in the project must be applied

Any design change = new cybersecurity analysis: Once you make a design change this has to be re-assessed from the cybersecurity point of view. Sometimes design aspects may not seem to be related to a cybersecurity vulnerability, nevertheless they need to be taken into account and evaluated.

Upgrading the security of existing software products: Device protection is complicated due to the levels of interoperability with multiple items of software and hardware items. Here, the coordination needed to conduct patch management safely is very difficult to execute. Be sure to analyse the vulnerabilities discovered with spares, pumps with error coded passwords and open ports.

Drawing on his previous work in the area, Massimiliano Nobile notes:"We have experienced that you have to dedicate part of your effort to work on beta versions of OS. If you are using IOS for example, or Android, you have to follow what is happening in the beta version and work in advance to new security features that are going to be released.

"In parallel, you have to work in the early stages to recall [and] upgrade functionalities. From the first day you have to know how to block usage of your product if something in the security is not okay."

Security Risk management: Manufacturers need to be proactive with security assessments and may want to introduce limits on how devices can be connected. New market entrants can get ahead in the industry via deploying security best practises from the outset to avoid having costly upgrades. [6]

Access Control: This can be implemented to limit access to certain features. However, once control design patterns have been made these can be hard to re-engineer in an application. This means that the access map must be finalised early on in the process. [7]

Proximity controlled access and bounding could be useful to block remote attacks and web interface issues. Software can be implemented to prevent data leakage and identify breaches in regards to sensitive information.

Depending on the operating systems used, some legacy devices may not be discoverable by network scanning tools that identify cyber security vulnerabilities.[2]

Query Parameterizaton - A programming technique used to mitigate SQL injections. SQL codes inserted into a web application could result in a whole database being stolen, cleared or amended.

Protect Data Transfers: In the transfer of data, encryption should be considered, TLS for instance for layer encryption. Sensitive information should not be exposed in transit which can happen with temporary storage locations and log files that attackers may be able to access. 7 Mobile applications lack adequate storage mechanisms and can cause leakage of critical information. Therefore in its recent Top 10 proactive control article The Open Web Application Security Project declares that ideally data should not be saved on a mobile device.

Contingency planning – network segregation is an another apt defence tactic - this may entail local area networks and firewalls. Patricia AH Williams and Andrew J Woodward in their recent article [2] note that contingency planning includes business impact analysis, incident detection and response, disaster recovery and business continuity. Bolstering system resilience through a governance approach can be implemented at various levels in a manufacturer's hierarchy.

- IEC 80001-2-8 http://

Level	To focus on…
Strategic levels	Compliance with regulation, policy creation
Tactical perspectives	Proactive risk management
Day-to-Day operations	Deploying technical controls like encryptions regularly and utilizing mitigation processes in workflow.

Final Remarks

Cybersecurity in medical devices is a topic that is only going to gain more attention over the next few years. This being said, more spending needs to be dedicated to the cause alongside more focus on security the primary stages of software development for medical devices. However, cybersecurity isn't obtained via one approach or line of thinking but in fact a fusion of various channels which will constantly need to be updated

Take Action And Attend:

SDMD Software Design for Medical Devices Europe™

21st - 22nd February 2017 | London,

Ground-breaking innovations, cutting-edge ideas and out-of-the-box development techniques are making the medical device marketplace more competitive every day. At the same time, increasingly rigorous standards and regulations are making regulatory compliance more difficult than ever before.

New for 2017

- Workshop: Cyber Security for Medical Device Software

- Roundtables - Cyber Security – The regulations and guidelines

- CYBER SECURITY AND RISK MITIGATION -Section on Day 1:

Postmarket Management of Cybersecurity in Medical Devices – The FDA's New Guidelines - *Fergal Mc Caffery, Director of the Regulated Software Research Centre, Dundalk Institute of Technology, and Member, LERO*

A Challenge of Design vs. Security: Medical Mobile Apps –
Massimiliano Nobile, SW Technical Leader, Engineering & Design, Flex

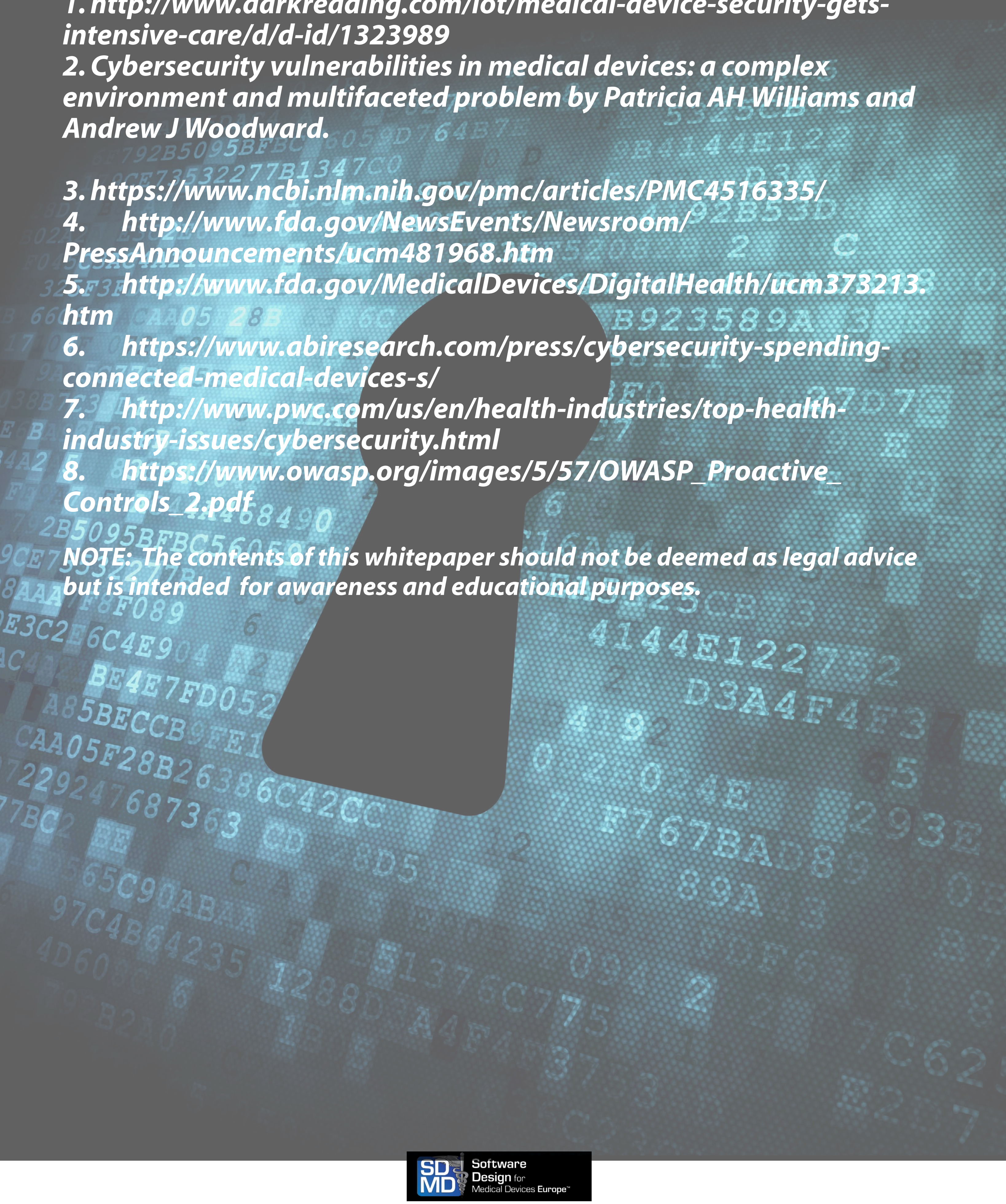
Safety First: Cyber Security for Medical Devices -
Pat Baird, Regulatory Head of Global Software Standards, Philips

Download Agenda

Call: +44 (0)207 036 1300

Visit: www.sdmdeurope.com

Email: enquire@IQPC.co.uk



Research

1. http://www.darkreading.com/iot/medical-device-security-gets-intensive-care/d/d-id/1323989

2. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem by Patricia AH Williams and Andrew J Woodward.

3. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/

4. http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm481968.htm

5. http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm

6. https://www.abiresearch.com/press/cybersecurity-spending-connected-medical-devices-s/

7. http://www.pwc.com/us/en/health-industries/top-health-industry-issues/cybersecurity.html

8. https://www.owasp.org/images/5/57/OWASP_Proactive_Controls_2.pdf

NOTE: The contents of this whitepaper should not be deemed as legal advice but is intended for awareness and educational purposes.