Q&A Session for
Medical Device Cybersecurity for HTM Professionals: An Update on Resources and Practices

Session number: 929858484

Date: Tuesday, September 18, 2018

Q: *Blue tooth is an additional option for connectivity, has this risk also been evaluated?*

A - Axel: Bluetooth vulnerabilities have been well documented, although there are certainly not as many as traditional network vulnerabilities. Also, it would be critical to understand the device's specific Bluetooth function (i.e. what is the risk, e.g. data privacy, or could the device function be altered) as well as the exploitability of the specific vulnerability (with Bluetooth being a short-range communication protocol, physical proximity to the device would be required).

I believe that several implantable devices like insulin pumps now use Bluetooth rather than a proprietary protocol. Obviously, this would need to be evaluated as part of the risk analysis and the manufacturer should be able to provide specific information on how Bluetooth risks are being mitigated.

A - Steve: Any connection whether it be by wi-fi, Bluetooth, infrared etc. should be considered in a security risk assessment as they all represent vulnerabilities and vectors for a security compromise. Refer to the device's MDS2 to learn the possible means of connection and examine how the device is being deployed and integrated in the clinical environment to understand and evaluate the relevant risks.

Q: *Every time I hear this discussed, there seems to be an implicit assumption that retaining and protecting legacy devices is more cost-effective than retiring and replacing them. Where is the economic analysis that supports this notion?*

A - Axel: I have not seen any economic analysis specific to legacy medical devices (I have seen a few that deal with the economies of cyber-risks in general, but that is a much simpler discussion). Clearly, this is a very complex question and may vary widely based on device type, use case, or organization. For example, the risk of a legacy MRI scanner would be quite different if an organization has just one (cyber incident would shut down all MR imaging) or several. Also, replacement cost may not just be the device itself (or sum of devices of that type) but also should include cost to backend systems, user training, potential downtime, etc. But either way, legacy systems should be identified because of their higher risk, and if replacement is not economic, compensating security controls should be put in pace (e.g. device-specific firewalls). Further, these devices should receive special attention on replacement planning as well as in the organization's incident response plan.

A - Steve: I don't believe there is universally correct answer as to whether it is either better security or more economic to replace/retire legacy systems or to retain them with added security safeguards (i.e., compensating controls). The appropriate approach when dealing with legacy systems is to evaluate the security risk they represent and consider the effectiveness and financial advantage of all risk mitigation options … including options to replace or the alternative of adding of security safeguards.

Q: *Wanted to say hello and I enjoyed your presentation. It has been a couple years. I am hoping to get my hands on a copy of your new handbook, and while I am not currently working on medical devices security here at the State of Michigan HHS it remains vital. Great job to the group brings back memories of the old working groups. Thanks for the opportunity to be brought up to speed on the latest information. Steve and I managed the HIMSS Medical Device Security Task Force and MDS2 development from 2002 to 2015, I was with VA at the time. Axel and I also worked together on some efforts and I presented with both gentlemen in the past. Thanks all.*

A - Axel: Thanks. Hope we get to collaborate again in the future.

A - Steve: Thanks. Good to hear from you. We have been doing this a long time, haven't we?

Q: *What special considerations are there for implantable medical devices regarding cyber security? What are current protective practices in implantables to restrict cybersecurity threats?*

A - Axel: Implantable devices are a unique category in the sense that on one hand they typically have a high risk of patient harm, but on the other hand they typically use proprietary protocols and patient proximity would be required – so, I could not launch a mass-attack against hundreds of pacemakers, I would need to attack one by one. From a risk analysis perspective, this would be a high impact but low probability (or low exploitability) scenario. A slight variation of this would be if we also consider the device-supporting infrastructure, for example a bedside station that would connect to the internet.

As for specific protective practices, this is probably unique based on device type and technology, I would like to defer this question to the respective manufacturers.

A - Steve: Many implantable devices are firmware/software based and can be programmed externally (e.g., implantable pacemakers, defibrillators, insulin pumps, etc.). The ability to affect the performance of these implantable devices by external means makes them vulnerable. An appropriate risk assessment should consider potential vectors for compromise (e.g., signals generated by a compromised programmer or extraneous signals from other sources) and take steps to mitigate the risk by adopting/employing appropriate administrative, technical and physical safeguards (e.g., training patients and clinicians in security hygiene, using VPNs on networked programmers).

Q: *There are a lot of statistics in this presentation that are great (40% devices connectable, 5% critical medical devices etc.) but there are no references to where that data is from. Is there a way to find out where all these stats are from?*

A - Steve: The number of critical devices (i.e., devices whose failure could reasonably result in death or serious injury) comes from my observation of how many hundreds of thousands of medical devices in hundreds of hospitals have been classified. For example, I have a list of over 700K medical devices from hundreds of hospitals that are maintained by one of the major independent service organizations in the country. Of those 700K medical devices, just over 26K (or less than 4%) were classified as critical by the hospitals according to the above definition. Given my experience, the number of hospitals and broad range and number of devices in this sample, I'm pretty confident that it is representative.

A 2011 Symantec white paper (*Networked Medical Devices: Security and Privacy Threats*) analyzed a survey conducted by College of Healthcare Information Management Executives (CHIME) of its members. That survey found 23% of medical devices currently networked and an additional 8% were network capable. We are speculating that 7 years after that survey was conducted that the 31% of networkable devices is likely now approaching 40%.

A - Axel: Steve answered this question.

Q: *With this significant disconnect between IT and HTM, we obviously need to address training and awareness. HTM schools or training organizations should include cybersecurity in their curriculum. Can AAMI offer this baseline cybersecurity specific training? Perhaps online to reach larger audience?*

A - Steve: We're very much in agreement. Axel and I are working on a university-based curriculum for CE's (starting at UCONN) and Barbara Christe has developed a medical device cyber curriculum for technicians/technologists at Indiana Purdue (IUPUI). AAMI is also looking at a certificate educational program.

A - Axel: This is an identified need and the recently published AAMI Guide was a first step, but we are working on additional offerings, as outlined by Steve.

A - Danielle: AAMI is aware of the knowledge gap that exists in the HTM community around cybersecurity. AAMI is in the process of creating a road map to bolster and strengthen HTM and education is at the forefront of this plan. AAMI will be providing more robust IT and cybersecurity educational offerings and content in the upcoming year.

Q: *Even vendor factory trainings should cover cybersecurity specific to their device. Is there a recommended baseline/minimum knowledge for HTM professionals? Specific training, certification, school, etc.?*

A - Steve: The FDA is continuing to work with manufacturers to ensure cybersecurity is better addressed in the pre-market approval process and that better support is provided owner/operators in the post-market support phase of the life cycle. The aforementioned academic/training programs for clinical engineers and biomed technicians/technologists are designed to cover baseline needs. We hope to convince a growing number of schools to adopt the curriculum.

A - Axel: I would hope that such standards or guidelines for specific training on medical device security (for HDO's as well as manufacturers) will develop over time.

Q: *What is your position of probability with regard to medical device risk assessment? Impact is easier to determine but the probability of a vulnerability being exploited is not such a straightforward calculation.*

A - Axel: Very good point. I come from the cybersecurity space and there, because of the reasons stated, it is much more common to look at "exploitability" (how easy would it be to exploit that vulnerability) rather than "probability". As stated in the question, it is very difficult to use probabilistic predictions like "likelihood" to assess security vulnerabilities. For example, the CVSS (Common Vulnerability Scoring System, Mitre) as well as the FDA Postmarket Guidance both use "exploitability"

A - Steve: It is true that the *probability* of medical device cyber events is not intuitive and that thankfully there has not been a sufficient history medical device cyber events to give us a basis for predicting such events in the future. However, we do know that security compromises are on the rise and that medical devices do have many of the vulnerabilities that plague other computer platforms. The calculation of *probability* needs to be a "best guess" informed by our knowledge and that of other experts about the medical device vulnerabilities and its ecosystem. While initial "guesses" about *probability* may be highly speculative that's ok. You can be sure that your ability to accurately predict a *probability* assessment will improve with experience in the process.

Q: *Congratulations to all panelists, the presentations have been awesome, incredibly informative and useful! I live in Brazil, where medical device security is still being downplayed and ignored. Is any chance to get a copy of the slides PDF?*

A - Steve: Obrigado. The slides are available on the HTA website (www.HealthTechnologyAlliance.org)

Q: *Has UL 2900 has good adoption? Does it have a strong future or is there something else we should be focusing on?*

A - Axel: Within the healthcare space I am aware of one medical device that has been certified under UL 2900. But in all fairness, it is a relatively new standard and even more, a new approach to the problem that needs to be accepted by the markets. FDA has recently adopted UL 2900 as a consensus standard, that will certainly drive adoption.

Q: *One thing missing is a risk management approach from a network engineering perspective. Steve did a great job of addressing the HTM risk management steps, but what about network engineering?*

A - Axel: I believe that there should be only one risk management process for medical devices that encompasses both, traditional medical device risk aspects as well as cyber (network) risk aspects. The output of the risk assessment (i.e. the actual controls to be implemented) then could happen on different levels either owned by HTM or owned by network engineering (or ITSec).

A - Steve: Effective security management of medical devices cannot be the sole responsibility of one group (e.g., clinical engineers, healthcare technology professionals). Rather medical device security management must be an integrated element in an enterprise-wide security management program that addresses computer workstations, communications systems, environmental controls, servers, IoT used by staff and public, etc. The effective security management program coordinates the activities of those who provide support to all of these systems. Network engineering has got to be part of the security management team and that means it must be appropriately integrated into the overall security management process.

Q: *I would expect to see items like Virtual Private Network, Access Control Lists, Network Segmentation, Intrusion Detection/Prevention, stateful packet inspection, etc. as well as Security Incident and Event Management (SIEM).*

A - Axel: I agree that these would be examples of security controls and measures that can be put in place as an outcome of a medical device risk assessment. We did not get into technical details in this presentation, there is more in the AAMI Guide and maybe we should make the actual “how to” part of a future presentation.

A - Steve: These are all examples of controls and processes whose existence and implementation is evaluated in the risk assessment process and that are considered as a means of further control and mitigating identified risks.

Q: *How does the HTA plan to influence HDO/OEM boards and exec mgmt to sponsor and fund these recommendations?*

A - Axel: In the end it is all about education and awareness. As we (as the larger community) discuss this topic it is important that we also engage the non-technical stakeholders and engaging in a discussion that expresses the medical device risks as also being a business risk, clinical risk, legal risk, etc.

A - Steve: Through presentations like this, publications and white papers we hope that we can provide you with convincing (real) facts and cogent arguments that we can use to make our case to industry and you can use to convince top management of the magnitude of the risks and the resources necessary to address them.

Q: *Can you share what FDA is doing to speeding up the approval or reapproval of devices for OS changes? Suggest including someone from FDA/manufacturer in this panel to address these concerns and provide them opportunity to present their side of challenges.*

A - Axel: FDA does typically not need to approve any changes that are made for the purpose of addressing cybersecurity risks as discussed in the FDA fact sheet: https://www.fda.gov/downloads/medicaldevices/digitalhealth/ucm544684.pdf. Exceptions of when FDA involvement may be required are discussed in the FDA Postmarket Guidance.

A - Steve: It is a myth that the FDA must approve patches and OS updates. The FDA only requires notification (not approval) if updates are done to address an issue that otherwise could result in serious injury or death. The FDA requires approval of an update when that update results in new device features/capabilities.

Q: *How we can close a gap between IT/security and vendors that they do not approve patches in timely manner or not aware?*

A - Axel: I believe the FDA Postmarket Guidance gives HDO the right arguments required to discuss this with vendors. The document clearly lays out the expectations around vendor vulnerability sharing and patch release.

A - Steve: The best way to pressure OEMs and vendors into issuing timely vetted software updates and patches is to include conditions regarding the timely availability and application of these updates/patches in purchase contracts and subsequent responsibility agreements. The medical device owners should also have a formal process that proactively checks for known vulnerabilities and the availability of these updates/patches and that ensures their timely application.

Q: *Can you add third party solutions to Philips servers that are residing on hospital computers to get proactive updates?*

A - Steve: Updates to any medical device software or to software on systems interacting with medical devices should be cleared through the OEM.

Q: *I've seen 25% of medical devices networked & 40% of medical devices are networked on the slides?*

A - Steve: The 25% refers to medical devices currently networked (based on a 2011 survey that found 23% networked). The 40% refers to the network capable medical devices. It includes both networked devices plus network capable (but not yet connected) devices (based on extrapolation on same 7 year old study showing 31%)

Q: *I did not think you could do penetration testing with medical devices?*

A - Steve: Penetration testing may be done on medical devices but only in a test environment after clearing with the OEM.

A - Axel: Also, penetration testing should be part of the manufacturer's best practices and results should be, as needed, shared with the HDO.

Q: *Speakers nicely summarized the current state and what we know today, but what trends or opportunities do they see where we are making progress, or need more prioritization/push from HDOs...particularly as it relates to Manufacturer testing/approval of patches and the ability for HDOs to install agents on medical devices?*

A - Axel: Clearly, broad acceptance of best practices (e.g. patching) would be desired so that HDO's don't need to wrestle with each individual manufacturer to have reasonable patch compliance. Also, I believe due to the complexity of the ecosystem, we need to look at opportunities for process automation, e.g. around vulnerability sharing or patch distribution (not actual deployment of the device but distribution to the HDO and tracking of deployment progress).

A - Steve: To some of us progress seems frustratingly slow considering where the industry is now in its security preparations and that this was a problem many of us were speaking out about more than 15 years ago. However, like the hammer making progress pounding a nail, we do see a growing awareness with each conference, white paper, regulation and guidance. There is a growing recognition among security experts, OEMs, providers, and regulators that better preparation and coordination among these stakeholders on security features, integration and life-cycle management is necessary.

Q: *Axel, will you explain the updated FDA regulations?*

A - Axel: Appreciate the question, but that would probably be a presentation all by itself.

Q: *I can understand how within the hospitals, one can control the risks, but how do hospitals manage vendors who are responsible for bringing in USB drives and Bluetooth devices that are used to manually update devices?*

A - Axel: Nobody (manufacturer, service technician, or clinician) should plug unsanctioned USB devices into medical devices. The risk that they near malware is just too large, in fact, based on what I hear from HDO's, more medical device malware infections are due to USB data carriers rather than external attacks. There are systems available that can scan USB drives for malware but, in the end, you would still need to rely on people being disciplined enough to actually use them.

A - Steve: Medical device owners must establish agreements with servicers that ensure appropriate security practices (e.g., scanning USB drives and Bluetooth devices by those servicers on a periodic basis and/or when going on-site to service) and the owners should periodically audit to ensure their servicers remain in compliance with these practices.

Q: *How do hospitals hold vendors accountable to timely patching and updates of legacy systems?*

A - Axel: Include security requirements, be it technical security controls or security processes like patching, in all purchasing documents including contracts or RFI/RFP's.

A - Steve: Requirements for timely patching of medical devices should be addressed in acquisition contracts and in responsibility agreements that include vendor conditions.

Q: *What education to do you require for clinical/biomedical engineering and HTM professionals to become more aware of data security issues?*

A - Axel: To date there is no formal security program for HTM professionals, although some are in discussion. ISC2 has a healthcare-specific security certification (HCISPP – Healthcare Information Security and Privacy Practitioner). Although it is general for healthcare with strong focus on HIPAA, this may be a good start for many.

A - Steve: The level of education/training for HTM professionals should correspond to their level of security-related responsibility. Professionals with primary responsibilities for medical devices and their security management should have a broad and in-depth knowledge of the security risk environment, what an effective security risk management program should look like and how to implement and manage it. HTM professionals that do not have designated responsibilities in managing medical device security should still be knowledgeable about the issue, about their organization's security practices and about their own security hygiene practices.

Q: *I understand the need for aligning responsibility for IT and HTM professionals, but what are hospitals doing to educate clinical staff who are purchasing these devices on the basics of cybersecurity and data security risk?*

A - Axel: Clinical staff education is an essential part of any medical device security program, be it to raise security awareness around replacement planning and procurement, educate secure device usage, or be able to detect a device security incident. Also, increasingly, clinicians will be asked to support security incident response if medical devices are involved or may be approached by patients with cybersecurity concerns.

A - Steve: Hospitals should ensure that buyers of medical devices are aware of importance of security when considering their options and that those buyers collaborate with security experts to ensure that appropriate security issues are addressed before selecting and acquiring a product. The hospital should also ensure the acquisition process is covered in an effective security management program.

How do you go about checking mobile media and thumb drives that vendors bring in? What type of internal security policies should your internal HTM department have?

A - Axel: This can be addressed in part through procedural controls in combination with USB malware scanning devices.

A - Steve: Medical device owners must have required procedures for vendors that ensure they are taking appropriate security practices (e.g., vendors scanning their USB drives on a periodic basis and/or whenever a vendor goes on-site to service) and those device owners should periodically audit vendor practices to ensure they remain in compliance with these practices