Q&A Report:

Question Asked

It seems that security should not only "protect the device and data" but also "protect the network". Thoughts on that?

When it comes to availability, I keep wondering about the Baylor incident, where HDTV took out a bunch of VHF telemetry systems at Baylor. In today's parlance, that was a large scale denial of service event. This could be used as a DOS attack on any hospital still using this old-style telemetry. Similarly, it is possible to use a software defined radio to decode pager alerts. Is there anything in MDS2 or any guidance that helps hospitals understand that the security of old technologies needs to be addressed?

Love the addition of SBOM and detailed content on SW updates!

Do the MPII questions include disposal of wearables (don't assume that because the battery is dead that ePHI can't be recovered from the device.

How can an MDM implement a glass break feature and NOT create a vulnerabilty (anyone who knows that feature exists has access)

and don't buy medical equipment form an MDM that won't provide an MDS2

Is there a timeline for manufacturers to move to the new 2019 form?

You mentioned that the MDS2 is being used worldwide - I wonder as to disclosure is made mandatory within regulation, or is it just voluntary for manufacturers at the moment?

Will the slides be made avalible?

For complex devices there are some questions that apply to multiple features or interfaces like TXCF-2 "is PII encrypted on the network?" The answer is "Some are, some aren't" Should we say "Yes" and then list the ones that are / aren't in a note?

what are the types of information that would/could be updated by an OEM on a MDS2 form? And how would a HDO know something was revised that they would need to be aware of?

Large established medical device OEM's are knowledgeable, aware and engaged w/ MDS2. Small or new OEM's, in my experience, are unaware or unfamiliar. Requests for a completed MDS2 form often requires coaching. Are there sources for training, self-help or external resources/documents for new users? ...especially in view of the expanded number of questions in the new format?

Do you feel compliance with MDS2 may be affected by the unwillingness of some device manufacturers to supply repair/service manuals. Is it a mandatory requirement for manufacturers to supply operating system requirements, upgrade info &/or the ability to make changes & upgrades even if a service manual isn't provided?

In your opinion, how should the MDS^2 change when submitting to other countires? for example, SBOM, various countries define Minor / Major SW change / verion differentely. Will this form need to be updted for each country we submit our product?

In your opinion, does the challenge reside on the OEMs to utilize the MDS2 or the HDOs to embed them as a baseline starting point? As the InfoSec team typically governs these processes within the security reviews and not typically HTM departments.

Is the MDS2 intended to be shared between HDOs/the public, or should it be not be shared due to sensitive information?

Do manufacturers have the residual risk file readily available to provide to HDOs? The AAMI medical device cybersecurity guide refers to this residual risk file

Are 80001-2-1/8 being updated to align with the updated MDS2 or should I say the standards still help to incorporate all aspects of MDS2

How much details to provide in a Sbom? Hundreds of libraries ? or high level? what are the recommendations

There’s a new version of MDS2 in town! What you need to know.

Answer Given

Yes, that is part of the network-level risk approach addresses by IEC 80001, and why the MDS2 sections are aligned with this standard. Protecting the network is more the responsibility of the HDO, and the information in the MDS2 is intended to help the HDO in evaluating the security controls that both protect the device and the network.

Addressing risks in legacy devices is a priority for MDMs, HDOs, and regulators. However, many legacy devices do not have MDS2s or other security documentation so the HDOs will need to work with the device MDMs to understand potential vulnerabilities and compensating controls that may be implemented. This topic would be worthy of its own webinar!

Glad to hear that, much effort underway to develop efficient and productive ways to provide that.

The MDS2 does not address wearable devices specifically, bit does address the capability of the device to permanently delete data (SGUD-2) and I would say that for a wearable that stores personal data, some additional info in the notes would be recommended.

That is true, of course a "break glass" feature is not really a security feature but rather an "anti-security" feature, and while this got some discussion during the update of the MDS2 it was decided that this was worthy of of addressing since for many devices certain security features can actually create a safety risk, and this feature would minimize that risk. Ideally the device with this feature would also include audit logs or other compensating security features.

May have missed part of this question…but certainly most device buyers are now asking for the MDS2 within the procurement process, and would need to consider some type of exception if a MDM would not provide one.

No defined timeline, the transition will be based more on indivudual manufacturers implementation processes, considering the various steps in the process as outlined in the webinar. It is reasonable to expect that the new versions will be available mid-year 2020.

Currently the MDS2 is not a regulatory requirement in any region, in all cases it is based on customer request.

Yes - The video recording of the webinar is posted online at www.healthtechnologyalliance.org. If you would like copies of the slide deck, please reach out to dmcgeary@aami.org

My recommendation would be to indicate "yes" and add clarification in the notes as you suggest.

The HDO would not update the MDS2 itself, this is based on the product specification as defined by the manufacturer. If a manufacturer upgraded a device such that new security feaures are added, a best practice would be to provide a new MDS2 reflecting the new software release.

Yes, smaller manufacturers are encouraged to participate in one or more of the various industry groups where best practices are developed and shared, such as MITA (for imaging MDMs) or H-ISAC. The number of MDMs with personnel focused on security has gone much deeper within the industry over the last few years, and I expect this trend to continue. As it does, more MDMs will have the capability to better address security and security documentation.

Could be a relationship here in that in some cases service information is proprietary and/or provided only after third-party service personnel have received the proper training. Similarly some MDMs could consider certain security-related information as proprietary or be reluctant to share specific security information so as not to disclose potential weaknesses. Sharing any design-related info (OS, SBOM, etc.) is not mandatory but rather recognized as an element of transparency, which will benefit the device owner/operators in managing risks. Some MDMs provide separate security manuals, and this wouldbe a best practice in cases where for whatever reason a service manual is not provided.

In my opinion, it is not practical for MDMs to have country-specific version of MDS2 (other than translations if that is necessary). The MDS2 is based on the device specification, and as long as the spec is the same, the MDS2 is the same.

The MDS2 is intended to be a mechanism to share information with the HDO (or other device owner/operators), and it is a good point that within the HDO security information can have multiple organizational audiences. From the MDM perspective, the MDS2 is intended to address the full range of considerations whether it be security as part of technology risk management, information security, or other. It is the responsibility of the HDO to ensure that the MDS2 is made available to all HDO users. Many HDOs, within their procurement process, have additional questions which can be a collection of questions from different internal organizations with different priorities. Of course, one of the goals of the expanded MDS2 is to minimize the need for additional information outside the MDS2.

Most MDMs do not make them generally available to the public, and provide them to HDOs for their internal use only and expect the HDOs to exercise the same considerations as with other business-sensitive information.

This depends on the MDM. Some have very comprehesive risk assessment and residual risk practices, and the intent to share this information with device users. Other MDMs do not have this maturity. As an industry our goal is to continue progression of industry practices in this area, and the MDS2 has been a starting point.

The update to IEC 80001 is independent of the MDS2 update, although my expectation is that the consistency in structure between MDS2 and IEC 80001 will remain. Note that we are not in a position to comment directly on IEC 80001.

My recommendation based on our experience is that the appropriate level of detail is at a higher level than the hundreds of libraries. At a minimum the SBOM must include OTS components, MDM-developed components, and any other software components with the potential for vulnerability discovery and/or patch requirements. However, more work needs to be done here, and I expect some years before we will develop a consistent and mature approach in the industry. This is also related to the difference in the quality processes between software and hardware, where the concept of a "BoM" is derived from hardware. Again, that would be another good webinar!