Additional Questions from interview with Kevin McDonald

(2/24/2021)

An 8-Year Journey to Medical Device Security — Lessons Learned

Q: What do you tell a hospital or health system that is still willing to ignore or delay the implementation of a good cybersecurity program to protect their networked medical assets?

You need to be able to provide to them the impacts on patient care, finances and institutional reputation. A key financial point to raise is the risk of losing hundreds of thousands of dollars a day if devices such as MRIs or CT scanners are inoperable, and your operating rooms are shut down. The UHS attack that happened demonstrates that this risk is not just hypothetical. They took a $67 million loss from their attack in 2020. I generally recommend using a business plan format that highlights a data driven summary about the risks and impacts that are possible where you are working and impacts other institutions experienced after such an incident. It is important to leave out "the sky is falling" and "cyber-Armageddon" comments.

One way to get the ball rolling is to perform a maturity assessment and bench marking with peers. (But the institution needs to understand it may not be acceptable for them to take a cyber risk just because their peers have.)

Q: If an event occurs, how important is knowing the detailed context of that device's location, authorized owner's name, software version, etc.? How can that information be located in a single trusted location for all devices?

As a foundation for your program, it is important to have a robust inventory that includes all of those data points. Right now, the best architecture I have seen is to use a passive scanning tool and intake processes to collect the data, and then replicate the data (all of it or subsets) into your enterprise inventory and into the CMMS that is used by your Biomed/HTM staff

Q: How much stock do you see our industry putting into the MDS^2, and how might you personally leverage this information within your program?

MDS^2 documentation has improved tremendously. I anticipate, as each vendor builds their library of MDS^{2}s for their products, they will continue to improve. The newest revisions are mapped to standards, and that has helped. We use the MDS^2 information as one more data point as part of our intake process. There are some key questions (such as the ability to patch software) that are critical to the risk of the device and it is managed. One thing to remember is that you need to also review the MDS^2 for odd answers. And build into your intake process documented steps about who and how the MDS^{2}s are reviewed and what you consider to be an "odd" answer.

Q: How do you correlate and then remediate an event across all potentially affected devices?

This is a fairly complex topic and books have been written about. At a minimum your institution should have a cyber security response plan that clearly lays out actions and roles for your IT managed devices. What is needed is to integrate your medical device response into your overall institutional response plan. Many of the tools used by your Security Operations Center are applicable to medical devices and attackers don't care if they move from a Windows-based medical device to an administrative assistant's laptop. It is important to be able to see and manage the full breadth of an event so your response needs to be at an institutional level and across all technology. Critical to your response (besides regularly practicing) is the involvement of your patient care staff, biomedical engineers and any specialized security staff. Your response plan should include who needs to be in the room and how to evaluate impacts of your response actions on patients and the patient care processes.

MedSec

inquiries@medsec.com
https://www.MedSec.com
+1.305.396.6900

Additional Questions from interview with Kevin McDonald

(2/24/2021)

An 8-Year Journey to Medical Device Security—Lessons Learned

Q: **How are expectations evolving for medical device manufacturers? To what extent, hospitals and other healthcare organizations expect device manufacturers to develop robust products from security and cybersecurity point of view, especially devices that rely on interoperability?**

Expectations have changed a lot over the last 8 years for manufacturers. Initially, it was difficult even getting an MDS^2 and when you did it looked like it was filled out by a summer intern. Now, most of the major manufacturers are involved, along with healthcare organizations, in groups such as H-ISAC, Archimedes and the Sector Coordinating Council. This puts them in direct contact with the security staff of their customers and allows a more open dialog on what is needed. Larger providers are setting and reinforcing the expectations on device security postures and on the ability to manage vendors' products. In my work with vendors, I've found it interesting that they have many of the same culture, skills, legacy technology issues that healthcare providers have.

Q: **Is H.R.7898 awareness being used in risk assessments?**

I am not familiar with any risk assessment that has used it. There has been work done based on 405 D (which the bill references) by the Healthcare Sector Coordinating Council. Resources for both healthcare providers and for medical device manufacturers can be found at https://healthsectorcouncil.org

Q: **For monitoring post deployment, do you see a future where regulations and the practices of the manufacturers changing to enable EDR style technologies to be widely deployed on medical devices?**

I have not seen any moves in that direction.

MedSec

inquiries@medsec.com
https://www.MedSec.com
+1.305.396.6900