10x Discussion on Medical Device CyberSecurity

**Presenter:** Suzanne Schwartz - FDA

In collaboration with [Joe Hage](https://www.linkedin.com/in/joe-hage) and the LinkedIn Medical Devices Group

---

**Suzanne Schwartz:** I’m going to frame this morning’s talk from the perspective of my role here at the Center for Devices and Radiological Health as the Center’s Emergency Operations Coordinator. And I’m going to tell you about our journey that has taken us from what was a very reactive stance to a much more proactive posture.

Last month, April, marks two years since CDRH became fully immersed if you will in medical device cybersecurity efforts.

In April of 2013, we were faced with a large packet of medical device vulnerabilities that were brought to our attention by a prominent cybersecurity researcher. This package span his spectrum from very low-risk medical devices to much higher risk one and involved many medical device manufacturers.

And we were essentially catapulted into response. Our FDA narrative on medical device cybersecurity at that time, [inaudible 01:21] was most keenly seen through the lens of incident or emergency response. Critical of course but really rather unidimensional. And yet, in the past 24 months, this story has really transformed to one of far greater [inaudible 01:41] and depth as a result of the multiple efforts that we have underway at CDRH to recognize the challenges for what they truly are. Panning the total product life cycle and across the entire spectrum of healthcare.

And so if you were to ask me today, May 5th, 2015 how I would characterize our medical device ecosystem within the context of cybersecurity of course, these are some of the descriptors that come to mind.

--------

[MedicalDevicesGroup.net](https://www.medicaldevicesgroup.net) • Join us at the **10x Medical Device Conference**, May 2-4, 2016 • San Diego
So these are some of the descriptors that come to mind. Complex, evolving, highly diverse players and stakeholders, many with competing needs and conflicting areas of tension, volatile, unpredictable and uncertain. There is nothing, absolutely nothing that is static about this space.

In fact, there are multiple moving parts. And we have to keep in mind that there are areas well outside of the medical device ecosystem in the broader universe, well beyond our control that are continuously shifting and these exert further influence or impact on the medical device ecosystem.

And so while our immersion has taught us an awful lot, we’re constantly uncovering war of the unknown [inaudible 03:38] incorporated in our thinking as we formulate that strategic approach for medical device cybersecurity.

A strategy that knits together the capabilities that FDA holds within its toolbox including policy through guidance, education, increasing awareness by outreach and communication.

So now that I have characterized the ecosystem, who are the players within it?

Well, we have obviously this audience, the medical device manufacturers with whom we at FDA have regulatory authority. And then there are the owners or operators and end-users of medical devices who we do not regulate.

As shown here, there are many players and many parties with a stake in this space. Whether it’s our patients, professional societies, industry, researchers, healthcare providers, venture capitalists. Within the bubble of healthcare facilities alone, we can further peel that back where we have hospital administrators, IT personnel, bio-med engineers, clinicians. We need not deliver the point then that vary and often competing needs among these stakeholders presents a significant challenge.

It would appear that a fundamental step would be to identify the coming interests that folks are able to rally around towards a shared purpose. The takeaway here though is that no one organization, no single government agency, no sole stakeholder, manufacturer, healthcare facility, provider, information security firm is going to be able to solve these issues on their own.

This requires what we consider a “whole of community” approach. Note that I didn’t say a “whole of government” approach because this is far more expansive than government alone. And so understanding the challenges, the hurdles and the opportunities to build creative solutions requires the ability to mobilize the community, the entire medical device ecosystem.

--------
MedicalDevicesGroup.net • Join us at the 10x Medical Device Conference, May 2-4, 2016 • San Diego
So for the remainder of my talk this morning, we’ll follow this roadmap. First, it’s about understanding the current landscape. What are the recognized challenges for enhancing security of critical infrastructure within the healthcare and public health sector?

Secondly, it’ll be about informing you about our medical device cybersecurity program.

And third, we’ll provide that glimpse into the vision ahead.

So let’s start with understanding the current landscape. We can ask ourselves what really is the scope of this issue within our nation’s health security. What is the exposure of medical devices to our healthcare critical infrastructure?

These CDC estimates speak volumes and I need not enumerate the actual numbers on the slide. Bottomline is that the majority of these encounters to date will likely include a networked medical device.

So let’s drill down a little bit into the considerations and challenges faced with regard to medical device cybersecurity. For simplicity, there are really two components to think about here. First, there are the characteristic of the devices themselves, these are more or less the intrinsic elements such as the fact that they contain configurable embedded computer systems. They are increasingly interconnected. Wirelessly connected. And then we have the entire challenge today of legacy device.

And then, there’s the use environment in which devices reside today. These are the extrinsic factors for which medical device manufacturers themselves really don’t have control. And some of the features that we are aware of and that we’ve come to observe and to learn further about within the use environment include the fact that there are varied responsibilities for procurement of devices, their installation and maintenance. Often these are silo-ed efforts within any one healthcare delivery organization and they vary from organization to organization as well.

Similarly, variable control over what is actually placed on the network and importantly, training and education with respect to security risks is rather inconsistent when you go from one Center or one healthcare facility to the next.

When we talk about vulnerabilities, the first thing to note and perhaps one of the most important things to kind of remember is that these are ubiquitous. One cannot entirely eliminate vulnerabilities. Yet, we can educate and we can increase awareness and vigilance among our stakeholder so that everyone understands what the common vulnerabilities are and what they can be doing to introduce protective measures.
We have in fact included the examples here on this slide in the safety communication that was issued back in June of 2013. And some examples are network connected devices infected or disabled by malware, uncontrolled distribution of passwords, a failure to provide timely security software updates and patches.

In our present landscape, there have been known incidents reported in the news and these are incidents related to malware. I want to be careful about making sure that the audience is aware that FDA has no knowledge of there ever having been an intentional exploit that was carried out that resulted in patient harm.

And so all of the references that I’m providing here with respect to exploits were done within a research environment. But with regard to incidents, the VA Cath Lab in 2010, there was a temporary closure due to malware infecting computers that are used for interventional cardiac procedures.

With regard to researcher demonstrated exploits, J. Radcliffe in 2011 demonstrated the capability of hacking an implantable insulin pump and as I referenced at the very beginning of my talk, in 2013, two security researchers, two prominent researchers, Billy Rios and McCorkle provided CDRH with a very very significant package of vulnerabilities involving medical devices that had to do with hardcoded passwords.

And over the past 12 months, there have been other researchers who have presented to us additional device vulnerabilities. These really become too numerous to list. Bottomline here is that vulnerabilities exist and the key is in developing the appropriate measures to assess the risk and manage the risk and to do so by adopting the appropriate tools, standards and best practices.

So with this, I’m actually concluding the background landscape of my talk and in the remaining time, I’m going to share with you some of the diverse and cross-cutting activities in which we have been involved at CDRH as we have looked to build out a much more formal and strategic medical device cybersecurity program over the past year and a half.

So what are our overarching goals?

Well number one, it’s to raise awareness with respect to cybersecurity in healthcare. And we do that through education, through outreach. We also importantly leverage knowledge from other industry sectors through their experiences. Whether it’s best practices or whether it’s experiences that they’ve learned from that we can translate to our sector.

-------

MedicalDevicesGroup.net • Join us at the 10x Medical Device Conference, May 2-4, 2016 • San Diego
Secondly, it’s about promoting the safety and security of medical devices in a forward-thinking way through the design of these devices by clear regulatory expectation.

Third, it’s about promoting proactive vulnerability management. And just to take a second here, I think that also what [inaudible 13:09] comes across within the theme of this talk is the dynamic and continuous nature, the total product life cycle approach with respect to medical device cybersecurity.

It doesn’t stop with the design. It doesn’t stop with the deployment of the device. It’s something that will require vigilance on a continuum.

Minimizing reactive approaches and then again that overarching thread that runs throughout all of these goals is that ability of fostering a “whole of community” approach.

Our cybersecurity program has included multiple efforts in parallel. We continue to articulate our current thinking for cybersecurity expectations through guidance documents. Our final guidance for content of premarket submissions for management of cybersecurity in medical devices was issued on October 2\textsuperscript{nd}, 2014.

I’ll spend a little bit more time on that guidance a little bit later.

So in 2013, we recognized 25 standards. These standards included both cybersecurity as well as interoperability.

We’ve issued public communication on the importance of shared responsibility in this space back in 2009 and more recently, that safety communication to all of our stakeholders in 2013 which included industry, hospital administrators, IT support, clinicians and bio-med engineers.

And organizationally, we established a Cybersecurity Working Group within the center of subject matter experts as well as having stood up a Cyber Incident Response Team under my program the Emergency Medical Countermeasures Program.

A few words about our CSWG that I’m very proud of, members of our CSWG had been involved in outreach, building awareness. Whether it’s through speaking engagements, the entire healthcare sector. The CSWG itself has also become increasingly educated and informed by our bringing in security firms and other experts who have presented their approaches, their perspectives and potential solutions to some of the challenges that we all face in this arena.

Importantly, the CSWG is tasked with evolving the agency’s thinking with respect to policy and guidance for the entire medical device product life cycle with respect to cybersecurity.

------

MedicalDevicesGroup.net • Join us at the 10x Medical Device Conference, May 2-4, 2016 • San Diego
And therefore, over the past year, we have been working very intently on the agency’s approach to post-market expectations and considerations for strengthening cybersecurity of medical devices that are in the field.

And so as one might imagine, these devices that are in current use present the greatest challenges for manufacturers and healthcare delivery organization with respect to vulnerability mitigation or mediation.

And this is in fact an illustration of where the complexity of the issue demands a multi-faceted approach.

To address medical device cybersecurity, we’ve engaged in a fair amount of collaboration and partnering activities with several of our federal partners. To highlight a few, as you can see here, we’ve built a relationship with DHS, the Department of Homeland Security. Specifically, their office of cybersecurity and communications.

And within that, what’s called the ICS-CERT team. The Industrial Control Systems Cyber Emergency Response Team with whom we engaged in incident response back in 2013 upon receipt of that package of vulnerabilities and with whom we continue to maintain very close coordination and communication at present. Having regular, actually weekly conference calls that allow both of our groups to maintain situational awareness on newly reported medical device vulnerabilities, potential threats and exploits.

We’ve also partnered, I want to draw your attention to the MOU, the Memorandum of Understanding with the NH-ISAC, the National Healthcare Information Sharing Analysis Center. That was executed back in August of 2014.

And the intent of that MOU is to develop a trusted environment for information sharing on medical device vulnerability.

Our collaboration with the NH-ISAC also aims to undertake adopting the NIST framework for improving critical infrastructure cybersecurity to medical devices. And therefore it would also include Cyber Incident Response Planning, Recovery and Resilience.

In the past few months, we’ve had the great privilege of seeing some of the early fruits of work born out of NH-ISAC collaborating with a group known as MDISS which stands for the Medical Device Innovation Safety and Security Consortium. This is a collective of medical device manufacturers, hospital [inaudible 19:05], bio-med engineers, security research firms and vulnerability researchers as well. As they begin to setup a feasibility small-scale pilot for medical

---------
MedicalDevicesGroup.net • Join us at the 10x Medical Device Conference, May 2-4, 2016 • San Diego
device vulnerability identification, assessment or analysis and information-sharing in a trusted space.

We are very excited about the prospects of this effort. And this is actually the perfect segue way to discuss work that we have ongoing with MITRE, our federally-funded research center with whom we have collaborated.

Our work with MITRE began in the fall of 2014. Again, MITRE is what’s called an FFRDC and they’re tasked with helping us at FDA advance the CDRH medical device security vision. They’ll do so by evolving a medical device vulnerability ecosystem that will share device vulnerability and other relevant cybersecurity information effectively and efficiently among both government as well as private sector stakeholders.

How are we doing this? Well to start with, through stakeholder engagement and in-depth interviews across the country, developing a roadmap for implementing the medical device vulnerability ecosystem that will reflect agreed upon shareholder roles and responsibilities and ultimately, where this gets to is that developing and designing a “trusted environment” for collecting, analyzing and sharing medical device vulnerability and security information.

So I’ve covered a fair share of FDA’s activities in medical device cybersecurity the past year leading what was arguably a significant inflection point for the ecosystem for last. Namely, the public workshop that FDA hosted in October 2014. This workshop that we convened was also co-sponsored with the Department HHS and Department of Homeland Security. We were beyond amazed by the number of participants within this workshop that included both on-site as well as remote participation globally that amounted to 1,300 attendees with a broad range of stakeholders.

The three overarching goals of this workshop were number one, to catalyze collaboration among all healthcare public health stakeholders. Secondly, to identify barriers that impede efforts towards promoting cybersecurity. And third, to advance that discussion on what are the innovative approaches for building securable medical devices.

The focus sessions of the workshop included increasing situational awareness, understanding what the gaps and challenges are and I’m highlighting here legacy devices as one of the key areas that presents a great challenge for us today. Exploring tools and standards, leveraging expertise and that expertise can be from well within this sector as well as expertise that comes from learnings and experiences of other critical infrastructure sectors. Whether it’s the financial sector or the energy sector or the IT sector. And establishing a collaborative model for information sharing and shared risk-assessment framework.

--------
MedicalDevicesGroup.net • Join us at the 10x Medical Device Conference, May 2-4, 2016 • San Diego
We took what we heard and what we learned at this workshop and we split it really into two big bins. What we’re calling systemic challenges in one bin and parenthetically it’s important to recognize that most of these themes in the systemic challenges, they’re not unique to healthcare and public health. They’re really universal to all sectors of critical infrastructure.

And then the second bin are the stakeholder challenges. Those that we would describe to the unique culture and entrenched behaviors of the community of healthcare and public health and its members.

So these are some of the things that we heard starting with the systemic challenges at the workshop. The cyber threat is growing. Cybersecurity may not be and is most likely not on the radar of the C-suite whether it’s for the manufacturers or whether it’s for the healthcare delivery organizations that remains a prevalent type of statement that we have heard.

There’s no safe space at present for information-sharing. There’s absence of a common taxonomy if you will or a lexicon by which to talk about vulnerabilities. There is something called the CDSS, the Common Vulnerability Scoring System and yet its applicability to date with medical devices has certain key entries that are lacking from it. And so this is an area of actually opportunity.

Lack standards for device integration and maintenance. There is no one-size fits all solution. We have large firms. We have small firms. We have the same thing to say about healthcare organizations as well.

And importantly, cybersecurity isn’t just a design issue. It’s not just at the time that the product is launched. It’s a life cycle issue. This requires a change in mindset.

Other factors that impose additional systemic challenge include what we observed and what we heard at the workshop about disjointed efforts across federal government. I suppose that that’s sort of a no-surprise but it’s an area that demands further work.

And healthcare and public health as a sector has been described as lagging behind by as much 10 years behind some of the other sectors with respect to advancing or improving, strengthening cybersecurity.

Though we are optimistic having seen some early signs that at least the level of awareness and understanding has increased in the past 6-9 months. With regard to stakeholder challenges, what emerged from the workshop were these findings. There’s a lack of trust, many stakeholders address cybersecurity in silos. Some don’t even understand really what the clinical
environment is all about. And so cybersecurity may be viewed within a vacuum and it does not take into account the context in which the device needs to operate.

Cybersecurity researchers bring disruption to the community and I want to make a point of saying that that is a neutral statement. Disruption is as much a good thing as it can be a negative thing and we see the enormous value and benefit that vulnerability researchers can provide to the medical device ecosystem.

But it is a shift in paradigm from how we thought about medical devices and their development and design and maintenance from where we were years ago. A lot of smaller organizations simply don’t have the resources or the expertise in order to be able to step up to the plate of medical device cybersecurity as some of the larger firms. This was another issue or another concern that was raised.

Stakeholders aren’t really sure how they’re supposed to prioritize vulnerability. They may not know all the present standards and tools that do exist. What are some of the good hygiene practices that could be employed that don’t require anything quite sophisticated?

And then very importantly, what is that value proposition for the C-suite in terms of making early on that investment, that careful intentional effort to make sure that our devices that are serving our patients have better cybersecurity?

One of the most compelling and unanimous sentiments that were expressed at the workshop by the close of day two was this desire to continue this important conversation. To take them to the next level. To use them as springboards for formulating tangible next steps.

And it was very important for us at FDA to commit to our stakeholders and to all the participants at the workshop that this one would be different. That this would not merely be a matter of people gathering for two days and then everyone’s going to return to their organizations and business would go on as usual.

There was a powerful energy in that room and we wanted to tap it and everyone wanted to be that energy sustained. So we knew we had to build on that event and we indicated at the workshop that we would find a way to create a space for continuing these important conversations. Recognizing that again, collaboration is at the core here of building that “whole of community” approach.

And so we therefore introduce the Handshake Virtual Collaboration Tool this past December, December 2014. The Handshake Virtual Collaboration Tool is administered by MITRE and it has been an enabling platform for ongoing discussion on topics covered during the workshop. Plus

--------

MedicalDevicesGroup.net • Join us at the 10x Medical Device Conference, May 2-4, 2016 • San Diego
new issues that people have brought forward and that can continue to be brought forward by anyone who is signed on the site.

And so this is our plug. First of all, we’re very interested in growing the number of participants on Handshake. This is the community’s site and it’s an opportunity to really provide perspective, provide concern and develop a means of collaborating towards developing solutions.

One can easily join by writing through cybermed.org or askmedcyberworkshop@FDA.hhs.org and request to be added.

Now, I can provide that information to Joe after the meeting so that anyone who would like to come on board with Handshake, we would be very happy to have you join the site.

Some of the recent topic areas which we have enjoyed really good discourse include cybersecurity of mobile medical devices, the Executive Order 13691 that was just recently issued on information-sharing and analysis organizations or ISAO’s as they’re called. Cyber Storm 5 which in its planning phases right now for February of next year 2016 and for those who may not be aware, Cyber Storm 5 is going to have a focus on the healthcare public health sector specifically looking towards scenarios that involve exploit of a medical device or other network systems.

And so we encourage the private sector to participate in these exercises as a means that will help further inform the types of measures and mitigations and preparedness that we need to be putting in place.

Legacy device is another topic that’s also been discussed on Handshake.

So I’d like to now pivot for just a few moments to underscore a few key principles of a final guidance that we issued on October 2nd, 2014. The title of that guidance is Content of Pre-Market Submissions for Management of Cybersecurity Medical Devices.

Again, FDA recognizes that medical device security, a shared responsibility between stakeholders. That includes healthcare facilities, patients, providers and medical device manufacturers.

Cybersecurity should be addressed during design and development. Again, the very concept of let’s bake cybersecurity in not bolt it on which is a problem that we actually face today with many of the legacy devices.

--------
MedicalDevicesGroup.net • Join us at the 10x Medical Device Conference, May 2-4, 2016 • San Diego
Design inputs related to cybersecurity should be established for devices. Similarly, cybersecurity vulnerability and management approach needs to be part of the software validation and analysis. And that’s required by 21 CFR 820.30(g).

This is part of design controls of the quality system regulation. The guidance aligns with the NIST Cybersecurity Framework 5 core functions. We discreetly call out these functions as identify, protect, detect, respond and recover and we encourage medical device manufacturers as they look to their development to adapt these five core functions as well.

It’s important for manufacturers to carefully consider the balance between cybersecurity safeguards and the usability of the device in its intended environment of use.

I can’t underscore this enough. This is to ensure that the security controls are appropriate for the intended users. No one, I’ll say it again. No one wants an outcome where the security controls hinder access to a device that is intended for use during the patient emergency.

So we have to be smart about these things.

And then the last bullet which is bolded very loudly and in another color to draw attention is one where we often are asked about whether additional submissions, new submissions are needed by medical device manufacturers in order to introduce changes, software changes for cybersecurity.

And so this is to once again debunk that [inaudible 34:46]. As is stated in the guidance and as is stated in prior guidance and many rare communications, FDA typically will not need to review or approve medical device software changes made solely to strengthen cybersecurity.

And now, wrapping up with this last slide which is ‘What’s our Forward Looking Vision?’ And this is a perfect note to end on because it not only provides a perspective for the future but it underscores that vision as being highly contingent, highly dependent upon the engagement and the collaboration of you, of our stakeholders, of the device industry, healthcare organizations, federal partners, subject matter experts, researchers.

As you can see, this is a continuous cycle. As I said earlier, nothing’s static at all about it. But that we hope and that we expect that through these collaborations, that will enable a platform for maintaining awareness of what are unintentional threats as well as those that could be intentional. It also informs or drives for us that regulatory clarity.

What are the pre-market expectations as well as the post-market ones? And it will further drive or fuel the post-market surveillance mentioned.
So with this, I would like to end the formal presentation and I think we have some time. I welcome the opportunity for some questions. Thank you.

**Joe Hage:** We sure do. Thank you. Let’s hear it.

*Applause*

**Joe Hage:** Now, in this unusual situation where it’s polite to put my back to you and talk to Suzanne, if you have a question in this case alone, I’ll ask you to come up here and talk to my computer so she can see you.

I’m going to ask the first question. Actually more of a statement.

First, thank you very very much. I know how busy you are and what we had to go through to get you to join us today. So thank you.

**Suzanne Schwartz:** My pleasure.

**Joe Hage:** First, next year, I’ve already began planning next year’s presentations and Mark Goodman the author of ‘Future Crimes’ agreed to speak with us and reading that book and seeing how incredibly vulnerable we are as a society is frightening. And he made a point that really stuck with me. He said that it’s financially equivalent to being ten to twenty times worse to have your medical records stolen than your credit card stolen.

Still, I find in my group and you pointed this out in the presentation a degree of not apathy but confusion/that’s-not-really ... you talked about silos, who’s really responsible for this?

I guess my question is a really broad one and that is, education programs like this one, I’m going to share this with the worldwide group, what do you think it will take for the structural change to come about that entire organizations approach cybersecurity as part of the life cycle program?

**Suzanne Schwartz:** So I think that it’s not all that bleak. We’re starting to see organizations get together and self-organize amongst each other to establish networks that by coalescing or recognizing that we need to sit up, sit straight and take this very very seriously. Especially in the context of the breaches that have occurred, the very serious breaches within the healthcare sector this past year.

Breaches that have just increased in magnitude from the first one to the second one to the third one.
So the reality, the harsh reality is hitting while we obviously want to avoid, I know this isn’t really much of an answer but we certainly want to be in a prepared state and for it not to take the equivalent of a Cyber 9/11 to really mobilize people into action.

I think that we’ve seen enough sensible signs and as we continue to engage in these kinds of conversations, that helps to raise the awareness. It also helps to bring the stakeholders from again, the different parts of the ecosystem to sit together in the same room and to understand each other’s [inaudible 39:55].

So that instead of finger-pointing at each other and blaming for absence of cybersecurity or for the allowance of breaches, there’s a recognition of, we all have this problem. It is one of shared ownership and shared responsibility. Here’s what my limitations are. Here’s what your limitations are. Here’s what we could possibly work through together. And that’s something that we’re starting to see now.

And I think that that happening on both the private sector side as well as engaging public private. The various government entities working with the private sector in establishing a different model towards improving what cybersecurity needs to look like in 12 months from now and in 24 months from now.

It’s obviously not going to happen overnight. We’re taking this incrementally but I think that this past year has demonstrated for people again a rather rude awakening that this is for real, this is not just for shock value. And that we need to take heed and put even the simplest practices, the very fundamental ones in place.

Joe Hage: Thank you. Carolyn has a question for you.

Carolyn: Good morning. Yes. That was a good segue way when you were talking about the private sector. Could you speak a little bit more about any kind of collaboration that is going on with the tech sector, with the Mandiants, the RSA’s, the FireEye’s and any of the tech companies, private sector tech companies? Is there a collaboration that’s going on with institutions and agencies like yours? Like the FDA?

Suzanne Schwartz: So we hear about a lot of efforts that are again, I would call them naisant with respect to the different security firms working either directly with medical device manufacturers as well as bringing on board healthcare delivery organizations so that you have nearly all of the appropriate parties at the table and when I talk about them sort of self-organizing, we’re starting to see different efforts become more visible.
What will be very helpful is if as these efforts continue to grow that either they continue to coalesce or potentially recognize what the niche areas may be so that there is a coordinated approach identifying and therefore working on specific gap areas.

My wish would be rather than seeing a lot of duplication and redundancy among efforts that we have a coordinated way forward and that expertise that might reside within different elements of private sector can actually partner up or link up with other parts of this sector or with the government through various grant and solicitations and announcements towards working in a more uniform manner to the end of again improving cybersecurity.

Joe Hage: Me again, I have another question. I know that one HIPPA violation is really expensive and that when an organization gets hit, it’s a potentially crippling, bankrupting amount of money in fines.

So I personally am not aware of any company that’s gone out of business because of it. I think of Primera that just had I don’t remember how many million records compromised. What really happens in those situations?

Suzanne Schwartz: Joe, not really sure I understand the question. Can you repeat that?

Joe Hage: Yes. My question is, with each HIPPA violation being such a burden on a company in terms of cost, are we seeing that in the real world where someone like the breach that we saw at Primera, Blue Cross that that kind of tax being levied on the offending or the hacked company? Is that a reality? What happens next?

Suzanne Schwartz: So I think that’s a little bit tough for me to answer. It’s not within my scope because as you know, FDA does not really ... is not involved on the HIPPA, breach of privacy violation side and to the extent that it would be a little unfair for me to comment on the question that you’re asking there.

With respect to medical devices, we are attempting to monitor that through intelligence and other means carefully with regard to any potential threats and what that cost could potentially be like for the public or the public health is obviously not merely a monetary cost but a cost to patients’ lives. That is primarily the area where we at FDA and specifically the Center for Devices is sharply focused.

Joe Hage: Thank you. Rendell has a question.

Rendell: Morning Suzanne. I’m Rendell [inaudible 46:02] with Arxan Technologies and we’re one of those private sector security firms that focuses on application security mostly within
medical devices specifically on mobile devices and allowing large medical device companies to bring forward their solutions on a BYOD basis.

So allowing them to not just bring forward a blackbox but allowing their users to download and install class 3 medical device software on IOS or Android. And we’re working with some very large entities to help do that and we’re actually working with one right now on a pre-submission.

So it was interesting to read the latest guidance and there was guidance around mobile security put out a couple of years ago as well. I guess I’d like your feedback on how best for a small security company like us to interact with the FDA and to get more exposure on how we can help the industry secure those medical devices as we are an ex-NSA/DOD company and are doing this and many other industry sectors as you pointed out indeed the medical device industry on a whole is certainly lagging insofar as adoption of some of these advanced software security techniques.

Thank you.

Suzanne Schwartz: And so I would welcome the opportunity for you to interact with first of all with us the Cybersecurity Working Group at CDRH directly. I think that that’s an important opportunity for us as well as for you to first of all for our being educated on the technology and the work that you’re doing and for our being able to also help guide the direction that you are seeking.

So absolutely first of all, the pre-submission process is always a way to go and I encourage you to do that but at the same time, in parallel or in advance of that, you can certainly reach out to me directly and we can set up an opportunity for you to brief our Cybersecurity Working Group on the technology and again the efforts that you have in place and how they interface with different medical devices.

Joe Hage: Thank you. It’s good to make that connection. I’ll be sure to put him in touch with you. Gary has a question.

Gary: Morning Suzanne. Gary Cohen formerly of Medtronic Diabetes. So I’m actually quite familiar with the Radcliffe issue that happened several years ago and also with what’s been happening recently with companies like Nightscout and I wonder what’s your view on how to work with basically the tech world out there that’s not really private sector, not really industry but those that are ... I don’t want to call them hackers because they’re actually doing good things but those who are trying to advance technology but aren’t under any regulations. How does the FDA look at them and how are they going to move forward in your view?
Suzanne Schwartz: Well you ask a multi-million dollar question there in terms of how FDA looks at things. So I would tell you that the FDA in our thinking about groups that are presenting information open source, doing work like Nightscout, we welcome the opportunity to engage with them and to have those types of discussions that will help all of us understand the various pathways forward. What might be the options? How we might think about those options going forward from a benefit-risk standpoint to the public health to the individuations.

This is ... when you talk about the ecosystem here being evolving and complex and uncertain, that’s exactly what we’re talking about. Newer technologies and newer ways of patients being able to monitor their health as well as family members being able to monitor their health in a manner in which no one ever conceived of years ago.

And so we want to be able to encourage that kind of advancement in technology. FDA of course does not want to be an obstacle or a hindrance to that. That thinking is an evolution in thinking and I don’t have an answer for you. I wish I did. Only to say that we would welcome as we have done those companies or those groups as they aren’t necessarily companies. But those entities, researchers to work with us to come forward and to request time to meet with us and to ideate on what might be some of the ways forward.

Joe Hage: Suzanne I know you have a hard stump, Neja has her last question.

Suzanne Schwartz: Okay.

Neyha: Hi! Thank you for your presentation. I’m Neja with the Healthcare Incubator and Accelerator called RedSky. I have a question, are we ever going to get ... there’s so much data everywhere and are we ever going to get to the point where the data evolves to develop an algorithm where we wouldn’t need security?

Suzanne Schwartz: Repeat the question? Was it the data evolves to a point where we don’t need security? Was that the question?

Joe Hage: Is the data going to become so smart that it develops its own algorithm that it doesn’t need to have security?

Suzanne Schwartz: Well that’s not a question for me. That’s a question for you all in the audience. I think that the developers are in a better position as subject matter experts and entrepreneurs and innovators to do that. The sky is the limit.

Joe Hage: I think that’s a fitting way for us to close. Suzanne, I’m very grateful. Thank you.

Suzanne Schwartz: Thank you.