Cybersecurity of Medical Devices: A Regulatory Science Gap Analysis

May 18-19, 2017

Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD, 20993

Day 1 May 17, 2017

8:13 a.m. - 12:27 p.m.

TRANSCRIPT OF MEETING May 18, 2017

TRANSCRIBER: JANINE THOMAS
NOTARY PUBLIC

(Proceedings recorded by electronic sound recording, transcript produced by transcription service.)

INDEX

INTRODUCTION AND WELCOME

EDWARD MARGERRISON: First of all, good morning and welcome to the FDA Campus into the very newly refurbished great room. Many of you have been in here before. I haven't been in here since my orientation about five months ago.

My name is Ed Margerrison. I am the Director of the Office of Science and Engineering Labs within the Center for Devices here at the Food and Drug Administration.

I wanted to welcome so many faces to this workshop and to make the only comment I'm going to make about the topical issue of the day. What a week to pick to have a cybersecurity workshop. Certainly very topical, but it's great to have so many people here and originally we weren't going to have quite this many people, but I'm thrilled that we do have about 300 attendees and I'm also absolutely delighted that we've got an enormous breadth of experience in this room and I think we've got all of the expertise that we need to make the workshop a huge success.

We've got clinicians and clinical practice.

We of course have industry both large and small. A lot of representatives from academia and also of course from the government. It's great to have you all here.

On the subject of government I'll also thrilled to be able to say that the FDA is co-hosting this with the National Science Foundation and also the Department of Homeland Security. Thanks for all your help and support in putting this together and I'm sure that all the attendees will have a chance to meet everyone as we go through.

One plea from me because we have more people that we were expecting, some of the sessions may get a little busy, so logistically it may be a little cramped. I still very much encourage everybody to participate as fully as they can. I think that's the only way that we'll get a really successful workshop. So some of the breakout sessions may get a little tight and a little busy, but please, your patience is very much appreciated and I think we'll have a great couple of days here.

So our aim during this couple of days is to try and identify gaps in our collective knowledge in the cybersecurity area and that is something that of course as I've said is topical, but it's also vitally important for us not to the NSF and the DHS, but also here at the FDA. Within the Center for Devices we are responsible for over half a million branded devices that are on the U.S. market.

We're currently seeing a massive increase in the amount of those that involve everything to do is cybersecurity so this is certainly not a theoretical issue for us. This is real and it's here today and we very much appreciate all your input and all your help in this.

The area of gaps in our knowledge we quite often call Regulatory Science and to explain that further I'd like invite my colleague Dr. Suzanne Schwartz up here to talk more about that. Suzanne is our Associate Director for Science and -- come on up Suzanne and Strategic Partnerships and she's going to explain that a little more fully and again, thank you all. Welcome and I hope you have a great couple of days. Susanne.

WHAT IS REGULATORY SCIENCE?

SUZANNE SCHWARTZ: Thank you. Thank you and good morning to all of our attendees at today's workshop on Medical Device Cybersecurity Identifying Regulatory Science Gaps and Regulatory Science gap analysis. I want to first begin by echoing Ed's opening remarks. It's outstanding to see such diverse representation and indeed it reflects first off the complexity of this space. Secondly, the recognition of its importance today more than ever and finally, number three, the need for a collaborative approach.

This workshop builds on our two prior workshops, our two prior public meetings that we had along that very theme of collaboration bringing the community together to tackle difficult challenges and having those difficult, but really necessary conversations on how we might approach these challenges to advance the posture of medical device cybersecurity within the health care and public health sector of critical infrastructure.

This workshop has however a very specific focus and that is on identifying, discussing and defining pathways or approaches to address regulatory science gaps in the area of medical device cybersecurity. And all of you, all of you who are here participating are uniquely suited to contribute your scientific, technical or clinical expertise to support this endeavor.

So what is regulatory science? Well, I'm going to take from our published guidance on that not our regulatory policy guidance, but of the documents that we put out which discuss what regulatory science is. We at Center for Devices and Radiological Health define regulatory science as the science in the service of regulation. What does that mean? Well, it means that it helps to ensure that regulatory decisions are well founded and that they do achieve the desired impact on public health by developing and applying tools, standards, methodologies to study safety effectiveness, quality and performance of medical devices and radiation emitting products under the total product life cycle framework. And we talk a lot in medical device cybersecurity about that concept of TPLC, Total Product Life Cycle and it's one that fits very, very much into today's workshop discussions as well, because it's surely about what happens in the design of devices and the testing of devices before they go on the market, but more so it's throughout that product's life cycle.

In addition, regulatory science facilitates good decision-making in the areas of, again, premarket evaluation, surveillance in the post-market arena, compliance and communication, so it embraces really broad range of disciplines, engineering, medicine, chemistry, toxicology, epidemiology, statistics, as well as the social sciences when we talk about regulatory science.

It's very much at CDRH aligned with and supports our center's mission and vision and therefore it has to be proactive and it has to be set up in a way that it enables anticipating what the regulatory and public health issues are so that we can also be responsive to emergent issues. It covers a breadth of research needs which of course includes investing infrastructure, but in addition to that developing evaluative tools, approaches or methods, addressing what might be long-standing questions such as concepts or topics that continuously might raise questions for our reviewers and addressing emerging issues.

Perhaps, perhaps the value add or said more strongly the criticality of regulatory science is no more acutely realized than when faced with an emerging public health concern. This is why when CDRH's Center Science Counsel our CSC went through the process of identifying the top 10 regulatory science priorities for the center for 2016 as well as for 2017 medical device cybersecurity is included within those top 10.

Events of the past week, the global impact of cyber-attack on critical infrastructure, the vulnerabilities of medical devices on connected systems and the real-time difficulties, I want to say that again, the real-time difficulties that health care provider organizations have in guarding against these kinds of attacks which can put patient safety at risk brings this message home to us today.

I want to take these last few moments to really applaud the planning team and give a special mention to our organizers Dinesh Patwardhan and Eugene Vasserman whose passion for this topic is really most evident in the stellar program that they have put together for the next two days, so please join me first off in recognizing their tireless work.

I personally as well as our broader team here look forward to the important discussions that we're going to have here over the next few days and I'm going to be paying close attention to all the insights and perspectives that are shared by each of you. Thank you very, very much. And I'd like to turn to Dinesh now.

WELCOMING REMARKS FDA.

DINESH PATWARDHAN: Good morning, everybody. Welcome to FDA. Let me add my warm welcome to beautiful words said by Ed and by Suzanne. My name is Dinesh Patwardhan. I am with the Office of Science and Engineering Labs here at CDRH at FDA. We just heard the regulatory science definition and over the next two days through discussion and dialogue we are going to analyze regulatory science gaps for this challenging and interdisciplinary subject of cybersecurity of medical devices.

Our goal is to publish a report later in the fall or the winter highlighting these regulatory science gaps. Our long-term aim is in this complex evolving and challenging field of cybersecurity of medical devices this report can perhaps highlight some common teams capitalize some solutions between different agencies and different stakeholders that are represented here today.

As was mentioned previously we have manufacturers which is critical. We also have clinicians, academia, independent experts and so on. So I welcome you to the workshop. I also want to focus on the breakout sessions that will happen here over the next two days.

First up we have plenary speakers. These plenary speakers will set the stage. These plenary speakers are this morning. Later on this afternoon is the breakout sessions. These breakout sessions, the topics were decided by input from the registration that we had from you.

The breakout sessions will have session leaders. These session leaders will catalyze their discussion, but each and every one of you needs to actively participate. We have very fortunate to have scribes or note takers. These note takers will take notes from the discussions in the workshop. These note takers, these notes will form the basis of the report that I mentioned earlier, so that active discussion in the workshop is very important.

For tomorrow the breakout topics are not very fixed. They are still fluid, that is because we are going to wait and see what are the discussions during the breakout sessions today and that will decide tomorrow's breakout topic, so each and every one of you, please join in and enrich their discussion of an ongoing topic or put a new topic on the table for the breakout sessions.

As was said earlier, some of these breakout sessions are at capacity. Your tags show what are those breakout sessions at the bottom. The challenge is we request, we make a plea that you stay with the breakout session. The breakout sessions chairs tomorrow after the second day breakouts in the afternoon we will all come together and we will hear the readout by the session chairs from all the breakouts, so if you miss other breakouts you will still understand what are the important aspects of the discussions that happened in other sessions, so we again, request you to stick with the breakout session that you requested to begin with.

And interdisciplinary workshop like this does not happen by individual, it is a team effort, I'm going to recognize my team here and I will call on their names and I request you to stand up and be recognized. First is Brian Fitzgerald of Office of Science and Engineering Labs. Paul Jones of Office of Science and Engineering Labs. Eugene Vasserman, Professor Eugene Vasserman is from Kansas State and he's on a sabbatical with Office of Science and Engineering Labs. Suzanne's group Seth Carmody, please stand up. He and Aftin Ross [ph] who could not be here today was very helpful, also very helpful in setting up this workshop.

In the program that you got, there is a slight correction. We have eight breakout sessions listed there. The first two and the second two, the first two and the second two they need to be combined. They will be in Room A and Room B, so as I'm facing it on the right-hand side is Room A and the left-hand is Room B. There would be a partition in here. So your tags are accurate, the printout is slightly has a typo. Outside the room you will find the accurate breakout session room numbers just in case you want to go outside and see.

As I said before, in addition to the FDA organizers, we have other agencies that helped out with the workshop. The other two agencies as was said before is National Science Foundation and Department of Homeland Security Science and Technology Director. These two agencies have been integral right from the planning stage to today. And Jeremy Epstein and David Corman from National Science Foundation and Daniel Massey from Department of Homeland Security. I request Jeremy Epstein to come up and say a few words.

WELCOMING REMARKS NSF.

JEREMY EPSTEIN: Good morning. Do we have slides up? If not I'll fake it. While he's looking for slides, the last time I was in this room I wasn't feeling well and I left early and this turned out to be a lucky thing, because those of you -- those people who stayed until the end got stuck in a magnificent ice storm and it took hours and hours and hours to get home. It took me 45 minutes to get home to Virginia, so it wasn't bad. So the message here is even though it's 90°

outside if you see me leaving early watch out for ice on your way home.

So while he's bringing up the slides, I want to also mention that when the slides come up you'll see my title and I was in a meeting recently where somebody told me that in Washington you can tell the importance of somebody by the length of their title. The shorter title means more important, like president. By that definition, I'm somewhere below janitor.

So Eugene Vasserman who is co-organizer of this event is one of our PIs at NSF and we're very proud of what he's done and we're very pleased that we were able to support his time here as a visiting scholar at the FDA and if any of the rest of you have NSF grants and -- thank you very much, Eugene. If any of the rest of you have NSF grants and are interested in being visiting scholars here at the FDA or elsewhere, please do talk to me. And you can see why I say the length of my title is inversely proportional to the importance of my job.

So at NSF we have two programs that sort of intersect covering the area of medical device security our SaTC Program Secure and Trust Worthy Cyberspace or for those of you who want to Google it, it's also Sex in the City, same acronym. And also our Cyber Physical Systems Program it's sort of medical devices are sort of at the intersection, so I'm just going to talk just briefly about each of those and I'll show you a couple of our sample research projects.

So this picture shows the scope of what the SaTC Program funds and the red box as you see there, interesting incompatibility between Macs and Windows it broke my letters and words in funny places. Anyway, so the medical device security fits into the Cyber Physical System's portion of this cybersecurity program as well as into the privacy program -- privacy year and a half within the program.

The SaTC Program just as -- it's the largest single research program in NSF. There's other programs that have more dollars, but they're building things like ice breakers and supercomputers, but in terms of research dollars SaTC Program is the biggest program at NSF. It has about 800 active research grants and covering the broad scope, so there aren't a lot of medical device projects, but there are some.

Within the -- our Cyber Physical Systems Program we cover, again the landscape of areas -- aeronautics, manufacturing, smart and connected communities, automotive, but as you can see one of them is medical and we cover medical devices in there, so it is definitely an area of interest for our Cyber Physical Systems Program.

I like this slide, kind of an eye chart, but this was from NSF CPS, Cyber Physical Systems Principal Investigators Meeting a few months ago and he identified why health care data is so hard to protect. I think the message here, I mean, it's not quite the same with medical devices, but it's pointing to the plethora of reasons, it's not just a simple problem.

The Thaw Program, Kevin Fu who's sitting here in the center is part of the Thaw Program. Kevin, are there any other Thaw researchers here today that you know of? Anyone else from Thaw here? So I mentioned that we have 800 research projects in the SaTC Program, of those 800 there's 7 that we -- that are our flagship programs, we call them our Frontier Programs and one of them is this one medical device security and this is a, I think it's a 10 million dollar, 5 year program. It's that order of magnitude and it's all about medical devices and also medical systems more broadly and their security. And you can see that nice picture of Kevin there in the lower right-hand corner and that'll help you recognize him at a break. And this is led by Dartmouth College, but a bunch of places involved also.

I think it's also pretty important to recognize, again, Kevin's work. Some of the earliest academic research if not the earliest academic research in medical device security was Kevin Fu's work on implantable devices, in particular defibrillator vulnerabilities. I remember when Kevin's work came out I went and talk to a friend of mine who's a cardiologist and I said, hey, have you read this cool paper? It's pretty neat and he said, I don't understand why would anyone ever want to hack a defibrillator and it really drove home to me the message that there's not only a technical difference between the communities, but there's a mindset difference of why would somebody do something like that and it's important to recognize not to say that one community is right and one community is wrong, just to say that we have to understand where each other is coming from to solve these problems.

I want to mention this project, this is also from NSF. This is a joint -- this one comes out of the Cyber Physical Systems Program, the others who I just mentioned came out of the Secure and Trustworthy Cyberspace, that is Cybersecurity Program and they're working on building resilient cyber physical systems for medical applications.

I need to opportunity out of course, Eugene's slide and Eugene gave me two different sets of text that I could use with this and I think the text I'm going to use is this whole project that he did or is working on it was his career award which I think I was the program officer who signed off on that which was kind of cool to watch my baby grow up and do great things here, but it's this sort of project that not only has done a lot of research, but it's also enabled him to spend this year here at FDA as a visiting scholar. And let's see, so you can see all the different work that he's done and how the research projects that he's been involved in are leading into standards and I didn't realize that was all animated.

We do have some solicitations on an annual basis. Our cybersecurity solicitation will come out in the fall, it's not released yet, but it always comes out sometime over the summer for submissions in the fall. And we welcome medical device research submissions from the academic and nonprofit communities. Our cyber physical systems solicitation comes out usually in the fall for submissions roughly in January, I don't know the exact dates for that. We're in the process right now of reviewing those proposals, but do keep an eye out for both sets of solicitations. And one of the questions that always comes up is do I submit to the cybersecurity solicitation or the cyber physical systems solicitation if I'm doing security of cyber physical systems like medical devices and the answer is, it depends.

And I encourage you to talk to me, talk to the program officers. It really depends on whether the focus, the innovation is in the cybersecurity side or whether the innovation is in the medical device cyber physical systems side like the control aspects and things like that. Which one is more appropriate, but by all means talk to us, talk to program officers and we'll help you figure out where the best match is.

And thank you again to FDA for organizing us and I'm happy I saw a couple people taking pictures not that there's anything very wise or anything like that, but if anyone wants slides I'm happy to send you these slides they are public information. Thank you very much.

DINESH PATWARDHAN: I introduce Dan Massey. Dan Massey is a Program Manager of Cybersecurity Division at Department of Homeland is Security Science and Technology Directorate and our partner in this workshop.

WELCOMING REMARKS DHS

DANIEL MASSEY: Great, thanks and following Jeremy's statement there about, you know, so incredibly long title which I think appropriately says something about where we fit, right. So let me pull up the right slides, he.

So we're really happy to be here and to be working with NSF and to be working with FDA. So I'm going to say a little bit about DHS, because NSF hopefully everybody in the academic community certainly has to be familiar with NSF. FDA plays, of course the key role in medical device regulation and regulatory science, so why is DHS here; right and I want to just spend a few minutes here explaining that and some of you already work with DHS, some of you probably should in the future and we'd love to kind of build those relationships. So I'm here at the Cybersecurity Division and these are the inputs we're looking at to say well, where should our priorities be; right? So we're partly guided by National Strategies to secure cyberspace to, you know, directives come out of the White House. There's a new executive order on cybersecurity just released within the last week or so. So we're guided by that. We're part of friendly DHS; right. So the TSA folks you see at the airport as well as, you know, FEMA, which hopefully you won't encounter and, you know, we're also the largest law enforcement agency in the country. And whether you put together Marshal Service, Secret Service, Border Patrol, ICE and so forth.

So we're supposed to be serving the cybersecurity needs of all those groups. We do a lot of interagency collaboration. The Cyber Physical Systems NSF Solicitation that Jeremy mentioned, we co-fund some of those projects, it's 90% NSF, but or actually probably more than 90% NSF, but a small part DHS as well and we've got some really interesting projects there, so if you are looking at this and you see, hey, I'm kind of mix of NSF and DHS there might be a way to get some funding in that direction.

We have 16 critical infrastructure sectors. So I'm hope -- I think I can -- I might already being able to claim this about medical devices, but one of my favorite statements is we also do automotive cybersecurity. We started it in about 2013 and here's a great stat. Since 2013 everything single vehicle DHS has produced is 100% cyber secure. Think about that; all right. So when's the last time you passed that DHS auto plant; right. We don't produce any vehicles. We don't produce any medical devices. We don't operate any financial systems. We don't run any of the smart grid, yet if any of these things suffer a catastrophic issue they're -- there's obviously national security and, you know, implications there and so we have a role, but an interesting role in that we operate any of it.

Finally, our last two and last, but certainly not least, state and local first responders. We're helping them with their cybersecurity missions and my boss Doug Mond [ph] likes to say cybersecurity is a global sport, every flag up here represents a company -- a country where either we are funding research in that country or they are funding research here or often both. So it's a big space, you know, it -- here's a little bit of the guidance. This is a bit old now, but this was the 2016, about every four, four to five years one of these plans come about and these are some of the areas that we're focused on that plan. This is still very valid stuff and worth taking a look at, but I point you more at the new cybersecurity executive order so I'll kind of skim by that one kind of fast, there.

So DHS in terms of our execution model, we're a little bit different than FDA. We're a little bit different than NSF. We are very focused on applied

R&D that's going to transition to practice; right. My boss, Doug Mond along with Dave Balenson [ph] who's here in the audience and a few other folks who are authors of Crossing the Valley of Death and that valley of death is taking that really cool research idea that Kevin or Eugene or any of you in the audience have and actually translating it into something that's in a medical device that I'm going to use or in, you know, in a hospital out into use. If you come to DHS and you say I've got a great idea for a white paper you're at the wrong agency. If you come to DHS and you say, hey, I've got an idea and I'll point to two examples here in a minute of some medical device research that if we could only get it past this stage it might be valuable to Kennett [ph], Boston Scientific or to a major hospital chain or there's a transition plan, that's where we want to be. We want to be in that space. And if you have some time, you know, fun reading on the plane ride home, you know, Crossing the Valley of Death it's a great article and it's generally about transitioning that R&D out into the real world. So that's kind of our model.

Last thing on our division and then I'll put up a few things of what we're doing in medical devices. So this is our mission, develop new technologies and techniques. This is hopefully applicable to a lot of what you guys are doing. Support technology transition. So the most important thing if you take nothing else away from this is DHS plus technology transition. If you come to us with a proposal that doesn't have a tech transition component it's dead on arrival, tech transition is what we want to do.

And finally, R&D leadership and coordination, you know, really, Dinesh and Eugene are, you know, 100% of the leadership on bringing this together, but we very much appreciate coming to events like this and helping to participate in multiagency things.

All right. So Cyber Physical Systems, I want to just say a little bit about that. So medical devices we would consider a cyber physical system, you know, Internet of things, cyber physical systems, smart community, we're not going to get tied up in the boundaries of what those things are, but our interesting concern here and it's not just medical devices it's our cars, it's our buildings, it's our smart grid. It's all these systems.

One of the Jeremy's formal colleagues Keith Marzullo [ph] at NSF used to say these are system you used to bet your life on and certainly our medical devices fall into that category. So it's very fast moving as you guys know. The field as we see it tends to be focused on functionality and patient safety and what we're worried about is when does security get added in and hopefully it doesn't get added in later. So we want to build that in now.

I'm going to have one more academic talk here on why do we need to build in security at this point? So this comes from Dave Clark at MIT. Dave's one of the founders of the Internet. This was published in 1988, but developed long before that and these were the design goals for the ARPANET which became the Internet; right.

So goal number -- I'm not going to go through all the goals, but goal number one, function despite the loss of networks and gateways. And wow does that work; right. I mean, if I pick up my phone right now I expect it to work. I expect to be able to make a call and that's not because cell towers never go down or routers never crash or anything like that. That's because the system was designed to work despite failures.

Goal number nine was accounting resources and I don't know about you, but I pay a flat rate at home for Internet and I suspect most of you do as well. And that's not chance; right. This is a consequence of the design goals and the ordering of the design goals.

So what Dave Clark has pointed out here is there's a design goal missing from this which is security; right. Not that we would have any cybersecurity incidents and the Internet certainly not in the last couple days, but Dave will point out that the failure, ability to work despite a component failing is very different than the ability to work despite a component being compromised.

If that cell tower fails, I'm going to roll over to one of three other -- I'm likely connected to three towers right now, I'll just roll over to one of them easily and I are won't even drop a call. If that cell tower is compromised and sending out bogus signals, all bets all off; right.

So the reason we put this up is so in the medical devices can anybody articulate and, you know, maybe this is something we can discuss in the breakout sessions. Can anybody articulate the design goals? Where is -- is security even one of the design goals? And if so, is it close to goal number one or is it close to goal number nine? And I think that's a really important thing to be looking at because otherwise just like the Internet we're going to design, you know, you guys are designing awesome systems. They are going to make incredible differences in people's lives, but if we don't put security in we're going to spend the next 20 years, 30 years or more coming back and saying how do we add security in later and we don't want to do that.

So last two things. What are we doing to help? There's a few, I'm just going to pull up -- point out a few groups in the audience, so Dale Nordenburg from MDISS [ph] is here. We're funding an effort on MDISS on a Medical Device Risk Assessment Platform. If you haven't seen that yet in one of the breakout groups, grab Dale, you know, Dale's got some great stats that should care us; right. That's a pretty large number; right. That's the estimated time a patient will be exposed to a connected medical device over the next ten years.

So we might say, you know, the odds of a cybersecurity incident may be 1, 2%. 1, 2% is a pretty big number, right, when you're talking about that number of interactions; right. So, you know, and this is an example of the kind of work that DHS funds. The medical device risk assessment platform fits in a bigger environment to really help device makers, hospitals and medical practitioners understand what the risk is, because we all know we're, you know, tech transition is very important for us. To say we should make the devices 100% cyber secure is great from a security standpoint, but I suspect everybody from industry here is driven by very economic constraints and, you know, I'll -- to avoid picking anybody here in the automotive space we actually can make 100% cyber secure truck and there are some scenarios, transportation of nuclear weapons for example, where that's very important. And that truck only costs about $500,000; right. So that's not going to be the truck that is commonly driven. We don't want to be in that scenario in the medical devices.

I'll give one last plug for one last group and then I'll come off the stage here. So Adventium Labs, Tom Carpenter here in the front, we're funding some work at Adventium looking at a platform called Isosceles [ph] really looking at how do you design cybersecurity in the devices? Can you do the appropriate separation? So a key concept in cybersecurity is separation of the critical functions and the noncritical functions. Again, to avoid picking on any particular medical device, if I look at my vehicle, my antilock brakes have a different set of security properties than the Bluetooth connection that lets my play my music while I'm driving home. They're should be separation between those so that the cybersecurity in the -- on, you know, whether or not my Bluetooth song is going to play is different from whether my brakes will apply. Obviously there are similar connections that you can make inside medical devices, we'd like to say that wait a minute, let's thing through, you just, what are the separation of the features? Can we build that in? Can we build in requirements and so, you know, Todd Carpenter at the Adventium team can talk more about that.

Those are two examples of the kind of things we fund and with that I will just conclude on this side which is if you want to come and talk with DHS about R&D funding, about R&D projects, you know, this is DHS' version of a famous set of DARPA questions, the Heilmeier questions, you know, here's what we'd like to know and here's what anybody I think doing research should ask. So first what's the need; right? Who cares? How's it done today? What are you trying to do? Can you articulate your objectives without using a lot of jargon? And that's challenging for all of us; right. What's your approach? How long is it going to take? How much will it cost? You know, and very important for government especially for DHS, I'm reporting all the time on Dale and Todd about, you know, what's the latest milestone they've achieved; right? And sometimes that happens literally week to week; right. You'll go from one meeting to say, all right, this was milestone, later that day we'll have a different meeting and they'll be like, what new milestone has been achieved? And I'll be like, well, you know, haven't even had a chance to talk to them since the last meeting, but. But it's very important to have those mid-term and final exams.

Finally, don't forget the benefits if you are successful, what difference will it make? What are the risks and the payoffs? We are research, so if there's no risk and this is just guaranteed it's going to work you should do it and there's no role for us.

And then finally, you know, what's new in your approach and why do you think it will be successful, so if you want to talk to DHS we're here, we're -- thank you for letting us co-sponsor some of this work and with that I'll pass it over to the next group. Thank you.

DINESH PATWARDHAN: So we get into our main plenary speakers here. I hope with the welcoming remarks that you heard with the last three talks, you captured the essence of this where FDA is focused on the regulatory science gap. Homeland Security is focused on the product development and National Science Foundation is focused on the long-term research.

In this challenging area of cybersecurity of medical devices, all these players have to be together so that was part of our working together on the getting all the three players together on the workshop.

In the brochure that you got at your registration we have details about bios for all our plenary speakers. I'm not going to be reading out all the details. I'm going to be very brief in introducing our speaker. Our first speaker is Pat Baird. He's the head of Global Software Standards at Philips. Before that he was at Baxter and his MBA and Masters is from Northwestern. Pat Baird.

RELATIONSHIP BETWEEN SECURITY, PATIENT SAFETY, AND USABILITY

PAT BAIRD: Thank you. So I real ized on the drive in today that it was actually five years ago this June that I was really first introduced to cybersecurity for medical devices. I was at a small workshop with Ken and with Kevin and I was presenting one topic and they started talking about security and for me in my medical device history in designing things, what I cared about security was when I was making morphine pumps and there's opioid-seeking patients, they'll try to take and pick a lock and break into the pump and so the tools that they used were a butter knife and a pen. And so to this day, okay, I have to admit when security folks are talking about pen testing, yeah, yeah, this is the first thing I think of, right, because this is the first and apparently the tools have evolved since then with the kind of security that we're talking about here.

And so also I notices that, you know, my life in product design was largely around patient safety risk management operator safety risk management. It's hazards has its situations its sequence of events and then these guys are talking about vulnerabilities and vectors and exploit s and it's like it's a completely different language and that's a just a completely different world, but then the more and more I talked and understood I thought that oh, there's a lot of underlying principles that are the same and are applicable. The details can be different, but I think that there's a lot of similarities and so that's what I was going to take and talk about today was trying to help, you know, build that bridge between these different knowledge domains, because to me they all come down to risk management and when I think of risk management and think about Murphy's Law. Now, I know some of you that know me have heard this story before, but for folks that aren't familiar with Murphy's Law, you know, if anything can go wrong it will go wrong. And I was curious about where this came from so I did some digging into the history of this and this actually came from the very early days in the space race and they came up with a question saying how much acceleration and deceleration can the human body take? We're going to put these astronauts in rockets and we're going to parachute them back down. We don't know how much acceleration is still okay and keep the astronaut alive.

And so there was a grant. They built a rocket sled out in the desert. The principal investigator was an MD and although there were other volunteers the PI said no, I'm the only human test subject, you know, so you're making sure that it's right and it's good, because I'm the one that's going to get strapped in.

And to give you an idea of the kind of forces we're talking about is they'd strap him in, light off the rocket engine, get it up to speed, hit the brakes, the rocket sled would go from 750 miles an hour to 0 in 2.5 seconds; okay. And so as they were qualifying this rocket sled before the human use trials the brakes had failed and the rocket sled shot 300 yard off the end of the rail into the desert. So imagine being the guy that has to go up to the doctor and say oh, you heard about the brakes? No, we fixed that. No, it's better, now, it's -- no, it's dealt with now.

Captain Murphy, so there was actually a Murphy involved in this had a team of scientists and engineers and technicians and they were trying to incent new gauges, try to do a better job at measuring the kind of forces that these people were subject to and had a technician take and go install one of the new gauges and at a press conference, right, because the press can hear the rockets going off, you know, hey, we heard the rocket last week, what did you find out? And how did it go? How did the new accelerometer perform?

So Captain Murphy gets up in front of the press and says I have this one technician, okay, he installed it backwards, so we got absolutely no data from that rocket run. Now, can you imagine having to go back to the doctor and say, hey, yeah, we got it backwards and so can you get back in the rocket sled and we can go try again?

And so Murphy was relating that there's this one technician. If there's a way to do if wrong he will find it. That was then quoted -- yeah, I know, we all know people like that; right. That was then quoted as Murphy said if anything can go wrong will go wrong. So you have to pause for a minute and admire the beauty that they misquoted the quote about getting things wrong; right, they got it wrong.

So anyway, to me risk management is about what are the things you're trying to do and how can things go wrong? It's all about managing how thing s go wrong regardless of if it's safety, if it's security, et cetera.

So a couple comparisons of just definitions of harm, the first one from the risk management standard 14971, talking about physical injury and then 80001 and then the recently published TR57, you can see in red where it just sort of adds and clarifies to me reduction effectiveness or breach of data and system security.

TR57 also takes and talks about the overlap between the security domains and the safety domains and some things are in between and there's even a, sorry for the size of the flow chart, but process flows saying this is how you do safety risk management. This is how you do security risk management and you know, you have to take the output of one and feed it back into the other. These processes are related. You can't do any of these in isolation without considering some of the other things.

I mentioned 14971, there was actually a periodic review of that standard performed recently and some of the feedback that they have and the 14971 team is actually working on this is to clarify. What is the relationship between safety and security when it comes to risk management? So that's still in the works.

But to me as I'm thinking about risk management and how I teach risk management, I actually break it down into just four steps regardless of terminology and domain specific things I actually found these four steps when I was doing research into retirement planning and the guide for retirement planning said the very first thing is write down what your goals are, I'm like, wow, you know, usually I teach my risk management of the very first thing is I start with my intended use. This is a much better description.

So these four steps, what is it you're trying to do for that thing that you're trying to do? What can go wrong? Is there something you can do about it? And then the last step which I think is really important is testing those things, those clever ideas that you had and seeing if they really, really work.

This I think maps nicely to the 14971 standard, those, you know, what is it you're trying to do? What can go wrong, did you do something about it? Some of those in between bullet points, right, that I don't have pointers to our go generator report. Go have a plan. Go do post-market monitoring of things. So I really like this model obviously.

Now, when I talk about some other

similarities, right, my wife is a technical writer, so it hurts me, right, to say that labeling isn't an effective mitigation, but so a couple observations from this photo, right, like, a) you don't have a sign like this unless there's been a problem; right. And then two, it's like you couldn't put a curb up or some rail or, you know, you can't have any other protective barriers in there; right. And then at one conference someone pointed out that the person in the wheelchair is texting for help, if you take a look at the silhouette, it was like, okay, well, at least there's that.

So another thing and I think of particular importance thinking about unintended consequences for I'm trying to design the safest thing in the world, well, doing that sacrifices a bunch of other things too. It's always got to be a balance, a tradeoff of different things. That's what engineering is about is tradeoffs and there's a really good book that was actually recommended to me by a doctor called Why Things Bite Back and it talks about sort of boomerang effects for good intentions and so there's a couple of examples that were brought up. One, which was I Guess North Atlantic

Fisherman is one of the most dangerous occupations you can have in the world, because storms come up quickly, you're caught out on deck and bad things happen to you when a storm comes out. So whether radar was installed in these and so the idea is you can see the storm coming that gives you time to take and get out. Unfortunately, it hasn't improved safety at all, because now the captain's stay on station as long as they can right up until the point where the storm hits and so there is actually no improvements in safety when it comes to this because people have adapted to the technology.

This other one I thought was interesting and so this book is a bit older. I know that car crashes have changed lately because of the cell phones, but this was interesting. There was a graph on how many cars, what percentage of cars in the U.S. have antilock brakes, because antilock brakes were introduced. It took, you know, a while for the majority of the cars to have ABS.

And then it was also a graph of the number of car crashes. And so you could see as the number of ABS cars went up a number of car crashes went down, but then they went back up again and are at the pre-ABS brake level and what happened was that now people are relying on their ABS brakes all of the time. They know it's there, they're not hitting the brake pedal until later and so it's almost like we keep seeking this one particular risk threshold that we want to have and even though we've introduced new technology, even though we're making the things safer, people manage to bring it back to where it was before.

So something I've shared with other groups is I became an engineer because of Wile E. Coyote, okay, between Legos and Wile E. Coyote. I wanted to help this coyote catch the damn bird; okay, right. And it wasn't until I became an engineer. I was going to help him, you know, build a better trap; right. It wasn't until I became an engineer that if you realize if you think back through, right, all of the plots, all of the episodes you've seen of this the failures are supplier quality related; okay, right.

So there was nothing wrong with the design of the rocket to catch the bird. The rocket blew up. So it's really about supplier quality on some of these things and I'm like, okay, well, how can I apply this lessons learned, it's too late, I'm an engineer, where do we need to take and focus things? Oh, guess what? Purchase components, software for non-profits, commercial off-the-shelf. That is a big potential source of problems for us both from a safety and security point of view and so it's up to us to make sure that those purchase components are doing -- I had also wondered, right, when I became an engineer why he didn't, the coyote didn't just switch to different suppliers; right. And because it's always Acme, right, it's always Acme and so I'm also thinking that maybe Acme's the only one that would extend credit to a coyote, right, or deliver in the middle of the desert in the 1970s, so anyway.

But when it comes around to SOUP and when different teams approach me saying well, we have these pieces of SOUP how do we manage it? What do we take and do with this? Is it okay? We bought it from somebody reputable. I take them back to the four-step process. What is the SOUP trying to do? What can go wrong and what's the consequences of the SOUP going wrong, et cetera, just walk through that.

And when I was writing software some of the platforms I was working on there were three to five pieces of SOUP. We'd buy a graphics library, a network stack, an operating system and that was about it. As I've talked to different teams over the years both inside my company and outside of the company, I've heard of products that have 40 pieces of SOUP. I've heard of products that have 200 pieces of SOUP. I've heard of products that have 500 pieces of SOUP; okay. And so I think that this is very interesting when it comes to SOUP management, we need to think a lot about patch management and obviously for security we need to think about patch management.

One topic that I'm trying to see if there's interest for do we need a white paper on something along these lines is when it comes to mechanic and electrical things, there's design for manufacturability. There's design for supportability. I'm wondering is there a need for some sort of something around design for patchability, design for up gradability [ph]. What are some of those best practices to manage? I understand how to manage when it's three to five. I'm wondering what are the best practices when it comes to 500. So I want to at least throw that out there.

I also wanted to stress the importance, okay, this is my favorite photo ever. The importance of verification and validation; okay. And so I'm pretty sure that there's a spec somewhere that says the barrier wall must stop a speeding motorcycle. It did; okay. Yep, it did, but I'm pretty sure there's an unmet user need here; right.

So when it comes to these things, yes, it looks good on paper. We implemented it. We tested it. Yeah, but we need to circle back to the user making sure that our solutions actually work in their world as well.

I also think that this person has great form, right, because I know I would be trying to flap, right, for this, because and I also hope that the helmet manufacturers understand the difference between verification and validation; right. And that will be tested in the next few seconds.

Also between both, you know, security and safety is you have to take a look at some of those near miss events; right. And just because it's a near miss, oh, no, it didn't hurt us this time doesn't mine you can ignore it, you have to go back and take a look at it, see what you can do to take and prevent that, as well as periodic reviews. We know things change over time. It's a different world than it was five years ago. And so even though the product meets all its specifications it might not need -- meet the needs of today, okay, when it comes to these things.

Now, of course, there's differences between safety and security and understanding those help me in my dialogues with my peers and so these are some quotes actually I had come across just in various standards meetings and people have made observations, so sorry, if you're in this room tell me and I'll cite you next time, but I thought this was interesting, safety is about keeping the product from hurting the environment; right. And security is about keeping the environment from hurting the product. Okay. That's a little different end of the telescope to take and look through.

Safety wants to make sure the product still does -- it does what it is supposed to do and security is making sure it still does what it's supposed to do even under some certainly trying circumstances and you can argue and talk about, well, safety has to, you know, if you drop the device it should still be safe. There's still some other things and completely understand, completely agree, but I think that a big theme of when you're doing these different risk management processes is where are these issues coming from? Outside the box or inside box?

When it comes to risk, it's really a factor of probability and severity and so let's look at probability first. A lot of times probability when it comes to safety is a factor of design. It's a factor of if you were manufacturing. It's a factor of your suppliers. And so these things are also easily estimated.

When it comes to security it's about motivation; right. It's about mayhem. It's about opportunity and so those things can be a lot harder to estimate. I can take and one of my devices throw it in a halt chamber and shake it at high temperature for a while, do some stress testing with that. It's kind of harder to understand the probabilities when it comes to security like that.

Also for safety risk management the probability is pretty constant over time, right. It might have some bathtub curves, but things are pretty predictable in how the life cycle's going to go, but with security, as soon as something's posted, as soon as someone finds, it, right, your probability goes from 0 to 100% overnight, well, less than overnight for that.

When it comes to severity, a large part of the severity is based on the intended use of the device. Yes, don't electrocute people. Yes, don't have sharp edges on your device, et cetera, some basic safety things in there, but a lot of the focus on product safety is about what you are, what the product is. With security a lot of times it's who you're connected to. So with security it's more of who you know rather than what you do.

Also, finally, I want to talk just a little about differences in human factors, because for safety risk management you want the easiest thing to use. You want it to be with a minimal amount of training and people to be able to take and use the device as needed, but when it comes to security, right, you don't want the easiest most usable thing when it comes to some of these topics and then I was actually take and close with this wasn't in the slides, but last week I was speaking at a nursing conference. A friend asked me to come in and teach them root cause analysis and quality management system kind of stuff and I was listening to the speaker before I was getting up and he was talking about risks in hospitals and talking about technology and talking about software and honestly, there was a lot of hatred in that room full of nurses and so this is -- there was 900 people total at the conference. There was about 350 people in the audience for this and there was venom is the best word that I can think of when it came to talking about computers in hospitals and the use of it and one of the big complaints that got some applause from the audience was when the speaker mentioned security in hospital systems and talking about the need to log into all of these different systems all the time and one particular cite that he was talking about it, it sounded as if and I might be getting this story wrong, but it sounded as if there was a bracelet that you could wear and walk up to a COW [ph] and one would automatically take and log you into the computer on wheels in the hospital and he was citing an example of a doctor coming up going and seeing the patient, walking back out to the COW, logging in, starting to put down a new order, oh, wait a minute, I want to check something, goes back in the room, talks to the patient more, comes back out, the computer is timed out, automatically logged him off, didn't save the intermediate order and now he has to do all the work all over again. And so the stupid software engineers, why do we need the security anyway? I am taking me twice as long to get this kind of work done than it did in the previous system, et cetera, and like I said lots of venom, lots of agreement in this. And I also could imagine, you know, a slightly different version of the story of I changed my mind and didn't go back to the computer and then when I went back three days later it had saved the order that I partially entered and so what a stupid computer. What a stupid piece of software. We need to do this and so I bring up this story, not just for like therapy from, you know, my brother in here, being someone persecuted in that audience, but also just we care a lot about safety. We care a lot about security and we have to also keep in mind how our good faith efforts are being perceived and figure out how we can better take and communicate these needs. Obviously, world events in the past week I think might be done some of that communication for us, but I also think that at the end of the day all of us need to do a better job of communicating exactly why we're doing some of the things that we're doing when it comes to this. All right. Thank you.

So in the original version of my slides, because I was unsure if there would be a Q&A period or not, I actually have and this might be why there's no questions. I actually have a flow chart of whether or not to ask questions during a seminar, because I know that, you know, the people in this room are very process oriented and so it's a little -- sorry, I can bring it back for you. Please go to the microphone.

UNIDENTIFIED SPEAKER: One of the real challenges with COTS and SOUP is of those 500 products that are in your product you'd probably find if you went to update them that 100 of the vendors have disappeared off the face of the planet.

PAT BAIRD: Yeah.

JULIAN GOLDMAN: A wonderful presentation. Julian Goldman from Mass General Hospital. I think a research question here is you pointed out towards the end of the presentation which is how can you understand enough about the context of use and the environment of use understand when you really should lock someone out of the computer or whatever the system is and, you know, we don't -- the systems today don't know whether someone is running in and out of the room and they actually have to keep checking something to complete an order list and you can think of that in other environments as well. So the fact that we don't have -- we have minimal information, we don't have rich contextual information. We have almost no contextual information from our clinical environments makes it very difficult to manage these security requirements and also makes it very difficult to play back and know what happened for future assessment if there is a problem, so we don't -- we don't have the context. We don't have the black box recorder and we don't have the ability to analyze that and I think those are some of the research questions I have.

EUGENE VASSERMAN: Kansas State University just a quick observation. We did some real-world observations and we found a security is -- even the same facility used vastly differently depending on the department and second, if you -- if you're introducing a security component into your product there's a very good chance to include side effects and communicate what a helpful thing you're security can be, so for example, what we found was that one department loved the security features, because they were -- who did what was automatically logged because they never have the time to do that themselves.

Another department left their machines logged in all the time with whoever's there and then spent hours at the end of the day reconciling their records and when asked why they said how else are we going to do it. So the -- their goal was already being achieved for them as a side effect of security. So I don't think I've ever published this anywhere, but I'm a big fan of some -- introducing artificial side effects into security whether they're really artificial or just appear artificial.

So I think the term I've been uses is value added security. That the security is actually doing something for you and whether that's a white lie or not I'll leave up to engineering.

DAN MASSEY: Dan Massey from DHS. So really like your comments about the patching and I think that's a fascinating problem. Do you have any view as to should patches be -- how do we handle the patches? Are these automatically pushed? Are these user driven? You know, this is a bit of a loaded question, but I thought I'd throw that out.

PAT BAIRD: So I believe that if you were to list all the different ways of those patches then you would have the answer. It's -- there's so many different business models. There's so many different architectures as it was I'll defer, open it up to anyone else that has a contrary opinion, but my experience has been it's everything. Yeah.

CHRISTINE SHERAPY: Christine Sherapy [ph] with Ark Devices [ph]. Curious about if there's any way to build in analytics to help with screening for security when there's abnormal behavior that's flowing to and from medical devices and if you could comment on that.

PAT BAIRD: I haven't met you before, but I'm a big fan of analytics. I didn't actually -- I don't remember paying you to ask about that, but I -- there's so many times that I've been able to take and resolve customer problems because of the analytics or black box and logs and being able to take in, so I'm a huge fan of having the analytics and data mining. I'm going to defer to, I'm more patient safety by visiting security places, so I'd really defer to other folks about their experiences when it comes to analytics and those kinds of implications, but love data.

KIRK HOLMES: Hi Pat, Kirk Holmes. You -- a lot of the anecdotes talk about people, but in your model that you described I notice that it doesn't really explicitly define the papal [ph] element, you know, the -- it's not just the products themselves.

PAT BAIRD: Fair enough.

KIRK HOLMES: But also of course, the people part of it, how people use it and that can be modeled and described and actually attached and I wondered if you thought about that and in the second common element that I always think is missed is you're a software guy, I understand configuration management with both safety and security seem to me that it always still comes back to making sure you have a good understanding of what you have goes back to your SOUP comment.

PAT BAIRD: Exactly, yes.

KIRK HOLMES: And without those kind of strong underlying processes, you know, it would seem that that would still be a challenge to address both safety and security and could be a common thread in those models too.

PAT BAIRD: I absolutely agree on the config management stuff. I was actually trying to keep the presentation just 15 minutes and so that's why I kind of blew through some of the things and left out a couple pieces. I completely agree with the config management and config management of your SOUP, right, as well as, what is that challenge, right, yeah.

My wife is actually whenever she hears me on a conference call, I work from home, she actually brings me a can of soup and just sets it in front of me when we're taking and talking about these things, but as for how are these devices used, yeah, I got a two-day training on that I give and absolutely agree I was fortunate enough about a decade ago to spend an entire summer just shadowing caregivers in hospitals, that's a whole lot harder to do now, but that was the best time of my life, understanding how much of a different world the caregivers live in than how the engineers envision hospitals and clinics working. I think that nurses has to be one of the most creative profession ever. I'd really like someone to do a benchmarking study just because some of the very creative solutions that came up with for little issues that pop up during the day regarding the patient, some of their very creative, very off labelly [ph] kinds of use of my devices and being able to take and see that in the real world and I think it's priceless when it comes to some of these things. Also back to, you know, Julian's comment as well. Okay.

DINESH PATWARDHAN: We're going to have one more question. This is the last question.

ADAM PORTER: Adam Porter from the University of Maryland and Frontal [ph] from U.S.A. and I really like to title of your talk which is about the integration, at least in my mind, the integration of safety and security. It seems to me that an insecure device is an unsafe device. Our -- do you know of or are you working on tools that actually integrate these two different models as sort of hazard models and security models and understand what is the impact of a failed security on safety cases and insurance cases and things like that?

PAT BAIRD: So I've done that kind of work in the past. Often I found it easier at least construction wise of having a security analysis over here and safety analysis over here, but then also making sure, you know, you're sitting in each other's design reviews or reviewing each other's documents to make sure you don't unintentionally add something in.

Of course one of the challenges is when it comes up to risk acceptability criteria and so, you know, I think sacrificing privacy versing killing someone, okay, I'm pretty clear on that tradeoff, but when it comes to a minor injury as compared to disclosure of billing records which I'm not sure there's any good guidance on how to do some of those other more subtle tradeoffs when it comes to benefit risk, but yeah.

ADAM PORTER: But I would offer at least, I think, sort of coming up with tools to look at these two concepts together. Might be an interesting gap in our technology. All right.

PAT BAIRD: Thank you.

DINESH PATWARDHAN: Let's thank Pat.

Our next speaker is Ken Hoyme. The title of his talk is Rumination on Challenges in Securing Medical Devices. Ken Hoyme is a Director of Product Security at Boston Scientific. This is his second stint at Boston?

KEN HOYME: Yes.

DINESH PATWARDHAN: With decades of experience in Honeywell and with Adventium Labs, so, Ken.

RUMINATIONS ON CHALLENGES IN SECURING MEDICAL DEVICES

KEN HOYME: While I get my slides up the other answer to the last question was to talk to Todd and

Eugene because there's some work being done at Adventium with Kansas State on modeling safety and security together. Okay.

So there we are. So I'm going to get some perspective having lived both the medical device world and in the research world of where I see from as a medical device manufacturer some of the areas that are challenging that might require some research.

I'm first going to wrestle with, you know, you chose a term rumination and there's really definitions, one is going into deep thought and the other is chewing cud and I will let you decide whether or not I've been chewing cud or giving you some deep thought.

One of a key problems that we have in this industry is scalability. We tend, I tend to mention that when we get together in conferences about cybersecurity in the medical device we have the big health delivery organizations talking to the big companies and there is far more small companies and far more community hospitals than there are the big ones and so as we wrestle with the solutions to these problems we have to think about are they applicable in an environment where I don't have a staff. I don't know Kevin McDonald's here, I think. I don't know how many at Mayo Clinic how much staff they have related to supporting the IT infrastructure and the security of things, but it's going to be completely different than the community hospital of 50 beds. So we need to think about that how that is that some hospitals will have great awareness of what they have inside their walls, others won't and one of the DARPA program managers that I worked with talked about success of a tool for DARPA is if it doesn't require a Ph.D. in the loop, so they have to be applicable by mere mortals.

A lot of words here, but bottom line is knowledge of what's in there, you know, in talking today with Phil Eglert [ph] before the meeting talk about and with the WannaCry hitting, you know, the first step that a hospital wants to know is, is it in their inventory what's there, so understanding what that third-party content is there's discovery tools out there, but they vary, obviously, you know, the understanding quickly I first heard this in heart bleed, it's like -- people with heart bleed can't -- not everyone wanted to know, or how many of my devices have openness of cell of that version in there.

So thinking about how you capture this, how you communicate this between manufactures and HDOs, how do you manage that understanding and if you want to get even deeper into it how do you decide what the impact is of a having a vulnerability, some vulnerability, not all vulnerabilities are equal.

Composability [ph] is another problem, so as a system engineer there's a lot of -- you know, understanding of what is an emergent property and both safety and security are emergent properties of a system, so and by emergent properties that is I can take a bunch of individually safe components and build an unsafe system and vice versa security of the same time.

So the nature of our system is that the FDA regulates devices one at a time. Each manufacture goes through and will present a case about why we think that device is safe and why we think that it's secure and then, you know, as Julian talks about with his ICE work and that the hospital will go and assemble them together at the bedside and now we're starting to think about more and more applications being -- what we want to do to monitor that patient at the bedside, who reasons about whether or not that collection of devices is still safe and is still secure? So it is not a necessarily a regulatory that you could argue that the assembly of multiple devices together to achieve another function is in and of itself a new medical device and requires it's on regulatory arguments, but again, evaluating the integrated safety and security of devices together in a way that can be done reasonably, potentially by staff within a hospital rather than staff at a company.

Same thing is with usability and I think we have a hybrid usability statement and this is, again, 6366 as a usability standard within the medical device space requires device manufacturers to do various kinds of evaluations of the usability of their particular device and present that argument as part of their overall safety arguments and then they're assembled together and the poor nurse has to figure out how and I looked at infusion pumps and the various different models and their complications and different manufacturers across all these various different device we start layering security requirements on top of these particular devices and each one is secured in a different way. Is patient harm introduced because of user confusion about how to unlock and how to access devices and so how do we evaluate the usability of integrated systems? What are the standards of things that we should be dealing with to make sure that collections of devices are collectively usable.

We get a lot of discussion about authentication. It is a very useful property to authenticate devices, again, whether you need to authentic a device when it's being used in a surgical room when everyone is scrubbed in and you have relatively good physical control of presence versus when they're out on the floor versus when they're in a nursing home versus, there's different use environments for the same device, but at the same time device manufacturers have to recognize that if you go into the clinical environment if you start introducing pins or passwords on things on devices that may be used in situation where infection control, where the nursing staff or the clinical staff are gloved or they've got face masks and you're going to do a biometric identifier from their eye and they're going into an environment where their eyes aren't directly visible, so we got -- thinking about the problems of how do we authentic in real-world environments and these kinds of medical devices and when is that appropriate and how do we do it is a hard problem.

We talk a lot about the need for break glass emergency situations and breaking glass in an electronic health record where you can do an expected audit of the record and provide consequences afterwards if somebody has been stirring through VIP records when they shouldn't have been, the consequence of that is fed back by that behavior, but if the device has implications on integrity and availability and essentially patient safety, does providing a break glass mechanism provide a mechanism to just bypass security altogether and it -- harm and how does is that balanced against the fact that the break glass is there because the device is needed in emergency situations, so again, reasoning about mechanisms to bypass security, you know, in a way that is -- has greater integrity than some of the mechanisms that may have been proposed before.

Machine to machine authentication. So there are certificate-based machine to machine authentications mechanisms, but again, there are the great thing about standards is there's so many of them. If we need to think about if we're going to place devices in hospital settings where the devices are going to interact with each other, they're going to interact with the electronic health record. As an individual manufacturer, I can come up with a solution for Boston's Scientific devices about how we're going to authentic, but if I try to introduce that into a particular hospital that may not necessarily be effective of what they're doing and hospitals may want to have the ability to layer their authentication mechanisms on top of it so that they don't know that isn't just -- they know that it isn't just an authentic Boston Scientific device authenticating, but it is an authentic Boston Scientific device that has been installed and configured appropriately for the Mayo Clinic so that when it goes on the network it's appropriately doing it, so what are the approaches and layers in this industry for getting machine to machine authentication done right and done quickly and effectively?

One of the things that was a surprising thing that I hadn't really gotten in -- learned about, but again, as Pat was talking about in terms of spending time in clinics, you learn things is leased devices, you know, they're -- I tend to think about individual devices it's an implantable device it goes in one patient and comes out later, but pumps and various other ones are leased and so therefore, in the process of transitioning from one hospital to another provisioning authentication credentials may be another aspect of how you condition them to be used in a -- the next facility, as well as from a security perspective the issue of being able to make sure that any PHI is removed from the device before it moves from one organization to another.

Dan talked about this in terms of separation. I come from an avionics background where the separation requirements for a commercial aircraft between software different safety critical levels was a fundamental requirement of the system. Boeing doesn't want airplanes to crash because as a fond person that Todd and I had worked with back at Boeing said is the -- if the toilet flusher control unit fails you do not want the plane to crash.

So looking at some of the separation technologies that have been developed and look at how we apply them better in the medical device domain, separation isn't necessarily just putting two things in two separate processes and running them side to side, side-by-side on a Windows Operating System, so there are architectures that can be done, but they are often still in a researchy [ph] kind of environment in getting them applicable so, again, we don't have the Ph.D. in the loop requirement is still areas where there's value and I think you'll hear one approach from Todd letter which is the Isosceles program that Dan talked about.

The other thing that drives me nuts, I understand it, but again, when I worked in the aviation world if you had gone no Boeing and suggested a Windows XP Operating System for the display units in their cockpit they would throw you out. They understand the lifecycle of an aircraft of 25 or 30 years and understand that the support cycle of that kind of cycle is not 25 to 30 years, yet we are so drawn in this industry of the low cost development of these kinds of commercial operating systems and I think we've seen powerlessness of many of the clinical IT biomedical engineers within hospitals as opposed to the bean counters and the people who push the cost, so there is this willingness to accept a device with an expiring operating system when the buyer knows for certain they're going to use it for 15 to 20 years. We need to think about operating systems that can be long-term supported that can be much simpler than the complexity that we put in that with complexity comes vulnerabilities, comes the need to patch more often and so certainly research into something that is still usable and cost effective and has support tools around it for being able to do graphics development and user interface that's the lure and development is, you know, the kids come out of computer science school knowing directly how to program these Windows kinds of systems, but there are certainly research needs for something that would be -- would fill that kind of niche in a way that's cost effective and in a way that's more long-term supportable. So I think that might be my last, so any questions?

PAT BAIRD: Something that I had been wondering and wanted to see if you had any thoughts or if this is a thing for, you know, a question for the larger group. Let me back up a bit, so for FDA's case for quality initiative, one of the things that we looked at was how to hold effective management reviews. And we wanted to provide a guidance on how to tell the difference between what I called management review theater which is where you have a review, there's costumes, there's props, there's a painted backdrop and there's a checklist and it says yes, I did all of these things. There, I held a management review, versus what one member of the team called endoscopic management reviews which I've never had to explain what that term meant, but what I've been wondering whether it comes talking about internal teams or I'm outsourcing a project or it's an acquisition or even for the HDOs is how can they tell the difference between cybersecurity theater and, you know, true cybersecurity. And so how do we know the difference between what's just dressing and what's real? So I don't know if you had any thoughts on that or if that's --

KEN HOYME: We were supposed to write a paper on that together.

PAT BAIRD: Uh, shit. Maybe that's why I remember it.

KEN HOYME: We've never gotten around to it.

PAT BAIRD: Oh, dammit. I withdrawal my question.

KEN HOYME: Yeah.

PAT BAIRD: Thank you.

KEN HOYME: No, certainly, I mean, I think it's at the root of that is how do you decide whether or not the cybersecurity controls that you're putting in place are effective and, you know, again, slapping a password on a system says okay, I've got authentication, but if the result of the password -- to me this is the connection I've always viewed usability as the third leg of the safety, we're getting into a lot of discussion related to safety and security and their relationship and the third is usability, so, you know, to your password post-it note is if the result of your security is, is that they end up putting the password on a post-it note then you really haven't done that security theater. Yeah, they're just sitting there right or under the desktop, because you don't -- that's the first place everyone looks for passwords. So, yeah, I think -- goes to another area might be are there effective usability techniques that allow you to assess how a system will get used in the real world and what the impact is going to be and if you go back to the Therac-25 story for those that remember that from the late 80s or 90s. Therac-25 was a radiation treatment machine that ended up killing several patients and there it wasn't a security issue, but it was ultimately a poorly designed software system that once the technicians that set it up got really familiar with it they started setting and typing the keys so fast that the handshake between a -- there was two processes that didn't have an interlock between them and when they out-used it that quickly corruption happened in the variables and because nobody anticipated in the design of that system that when people got familiar with it that's how fast they were going to be typing things in.

So similarly, in terms of how do you create the kinds of normally usability is done by going and observing, but if you give somebody a checklist they're going to do things in a different way than what they're going to do when they're actually -- become very familiar with it, so how do you assess security behaviors in a real-world environment? Eugene.

EUGENE VASSERMAN: Eugene Vasserman again, Kansas State University this is more of a chance to get a word in edgewise, I guess. It does connect back with your point about complexity unless I'm terribly misinformed and even if I am it will still make a good story. The fundamental reason for that race condition you just described in Therac-25 or at least the reason it showed up and again, I've learned all of this from third party sources, so I don't know if this is correct, is because a hardware interlock on the placement of the filter was replaced by air quote, software interlock and I really like the words of Drew Ray [ph] who used to do the disaster cast safety podcast that a dynamic system that requires many moving parts in order to work cannot, is not and never can be an interlock. So there is no such thing as a software interlock and Therac-25 shows us that very well and the reason for that is not because we don't know how to build software or interlocks, it's because there's so much complexity something sneaks in. There's bugs. There's more bugs in hardware I don't mean processor.

KEN HOYME: Yeah.

DINESH PATWARDHAN: Anymore questions? There's one more question.

KEN HOYME: Oh.

KIRK HOLMES: Kirk Holmes. I do want to ask you about your last slide where you talked about the OS and the lifecycle and what are your thoughts about the other approach of a more layered architecture where you separate so that you can basically separate the OS from user functionality from different functions so that over time you can upgrade the OS without having to do major changes to those architectural components. Just, you know, managing the interfaces?

PAT BAIRD: So, yes, I think separation and that, but I think if you -- if the OS is still really a complex OS in one of, you know, that's essentially like a virtual machine kind of approach to it in if you use a very simple OS in the things that are very safety critical and/or security critical and leave the more complexity for user interface or that you still are going to be getting into a patch management issue which is, you know, the more complicated a software you end up putting in there the more vulnerabilities that will be showing up in it and it will, you know, it will need to be updated, so it's a -- but yes, I think the layered separator architectures stay tuned after the break.

RUSSELL JONES: Hey Ken, Russell Jones, Deloitte has anyone ever approached from the industry like a Microsoft or an Apple to talk about a med device specific, kind of an OS? And I think the second part of the question is, is there enough of a market for a Microsoft and Apple to kind of say, oh, yeah, okay, that's something we would go do?

KEN HOYME: I have not heard specific to the medical world, but certainly as we look at the complexity of the IOT devices and the number of IOT devices this problem is ubiquitous to anything that's cyber physical that could have safety security implications, yeah. Julian.

JULIAN GOLDMAN: Great presentation. One of your earlier slides you pointed out that HDL's legitimately need to know the software version of their devices and the patch level and, of course, absolutely true. The interesting thing is the challenge of finding out even when calling manufacturers urgently to determine what the current version is some manufacturers are -- provide information on the web, others are relatively clueless about the products that they have in the market for whatever reason.

It's interesting that when we have other software products typical products we use everyday they usually check a server. They often check a server and they indicate right away whether they're out-of-date, right, we all see that everyday on our systems. And so in the spirit of framing the research questions here, how can medical devices do something like that and check their latest patch level, software version level and so forth in a safe and secure manner as do most other, you know, commonly used software COT's platforms today?

That certainly would help if it can be done and there are many products, for example, that routinely down check and download for the latest Microsoft security patches. One of the products that we use within partners, a very commonly used medical device automatically downloads the latest patches, I think you're well familiar with that and it doesn't install them, but requires a clinical engineer, a biomedical engineer to look at the service information from the manufacturer and then decide if it's appropriate, that it's been validated for use on the product.

So we're almost there, but it does seem that it's worth, you know, a research effort to find out how to make that ubiquitous.

KEN HOYME: I agree, some research is underway. I know under Dan's Cyber Physical Systems Security program there's actually, I think 10 different contracts under it and a couple of them are related to security software updating. It's not in the medical device demand, I think automotive has been one of its one, but I think the information from those projects as they come out it would be good to get circulated more broadly.

JULIAN GOLDMAN: Thank you.

DINESH PATWARDHAN: Last question.

DANNY BARTLETT: Danny Bartlett. Dense Supplies. We're talking about the software and the higher level firmware, but if you take a look at your phone and anything that's talking to the cellular networks, the chip sets and the modules are getting updated all the time without any notification to the user and it's it IOT, et cetera.

I do expect that how you want to -- how do you expect that to get handled or to get a handle on that because the network engineers are not even seeing this. This is being done just throughout the cellular networks.

KEN HOYME: It's an interesting parallel, because it's in an nonregulated environment the consequences of if an update causes, I mean, I -- for some reason, my kids when they update their phones have more problems with their phones than I do, but there are odd weird effects that do come up from updates and I think as we evolve in an industry that how we recover from things if they auto-update and something breaks it's -- but, yeah, there's certainly lessons from those kinds of industries that we can learn and try to figure out how we could apply.

DANNY BARTLETT: Thank you.

DINESH PATWARDHAN: Let's thank our speaker. So a couple housekeeping rules. We are coming up on a break. We are going to gather here at 10:15. The lunch if you -- our request is if you are going to purchase lunch here please go to the registration counter if you haven't done so and prepay so there's not a long line at lunchtime and you can have some discussions on the side lines, thank, we'll meet at 10:15 back here. Thank you.

- - -

Pause for a recess

- - -

DINESH PATWARDHAN: Please, can we get seated? We are getting started here. Okay. Let's get started. Welcome back. I hope you're having interesting conversations and some networking. That's the whole plan of this workshop. Next up we have a tag team from MITRE, Penny Chase is the Information Technology and Cybersecurity Technology Integrator at MITRE and Steve Christy Coley is the Principal Information Security

Engineer at MITRE.

Their title of their talk is using CVSS in Medical Device Security Risk Assessment. Once again I remind you that the details of their plenary speakers' bios are in the handout that -- when you got yesterday. I'm briefly introducing them, thank you.

USING CVSS IN MEDICAL DEVICE SECURITY RISK ASSESSMENT

PENNY CHASE: Thank you. It's a pleasure and honor to be here. So I'm going to go over first and then turn things over to Steve, so we're -- so just to kind of set the stage of what we're trying to do, you know, vulnerability is discovered and people are interested in understanding the severity and the potential risk and there are lots of people who care about this and they all bring different perspectives to it. So the vulnerability who discovered the vulnerability may be looking at the vulnerability from a purely IT technical perspective. What are the real technical impacts and they see something like, you know, no password access to the device through Telnet or something like that and that is just a bad thing from a technical perspective, but they don't necessarily think about it from the perspectives that the device manufacturer, health care providers and patient have, you know, the device manufacturers and that's not a monolithic entity even within device manufacturers who have different groups. You have, you know, the product engineers who have the safety and quality people. You have security people. You have privacy people. They're all thinking -- looking at this vulnerability and trying to figure out, you know, do I need to patch it now? Can I put it off for a routine maintenance upgrade? Do I need to employ some kind of mitigations? Do I already have mitigations in place? So they're thinking through those kinds of questions.

Health care providers, you know they find out about it and they're wondering, you know, is this something that's going to cause a problem for me, you know, how do I control this? Are there already compensating controls in place? Do I have to work with the manufacturer to figure out how to mitigate it? Do I just have to unplug it from the network? And patients, you know, especially when we had these newsworthy events, you know, WannaCry, other kind of things they might wonder what's the impact for me and my treatment and, you know, there's a potential of patients thinking that the security impact may overwhelm their, you know, their need for having us treatment. And FDA from the regulatory standpoint, you know, wonders, you know, is this something that is a regulatory concern? Is there a sufficient impact to safety -- patient safety and harm that we need to take some kind of action?

So this is our VEN [ph] diagram and it's interesting how we've seen some other VEN diagrams and we kind of realize this space is complicated. There are these different properties that we care about. We care about safety. We care about security and privacy and they overlap and interact in many interesting ways. There may be different regulatory regimes covering each of these and people need to understand that. These things may interfere with each other or impact each other in different ways, you know, a security vulnerability, I mean, somebody asked in the previous session or made the observation, you know, isn't an insecure system an unsafe system and in many cases that might be true, you know, security vulnerabilities may really have an impact on the effective performance of the device. On the other hand you may put security controls in place, you know, for example, you may want to run the antivirus on the device, but you may not want to run it while the device is being used during a surgical procedure and there was a report of that last year. Here, you know, we've put privacy in here, but our focus, because this is an FDA conference on cybersecurity and regulatory science, the real focus is on the interactions between security and safety.

So when you've got real-world vulnerabilities and you want to score them, there are challenges. It can be very difficult to determine what the safety impact of a technical finding is and you know, we've already heard I think, you know, folks in the previous session say, you know, you can't, you know, they may be different, you may do a security analysis and a safety analysis independently, you may want to figure out ways to combine them, but it can be very, very complicated.

We have for example, if a device has some fail-safes and if a vulnerability is exploited and it causes those fail-safe measures to kick in it may degrade the operation of the device, but it's something that the device manufacturer may have not thought about it from that -- from the perspective of the -- that a security vulnerability might have triggered it, it might have, you know, it might just be there for other reasons, but that fail-safe operation, you know, does that mean that, you know, how do you weigh that in determining what the real severity of the vulnerability is since, as I said, you know, intended to operate that way in the -- in unsafe circumstances.

The vulnerable applications might not actually direct with -- interact with physical actions directly, it depends on the functionality and the work flow, so, you know, you might, you know, there might be a vulnerability of third-party software that doesn't really have much of an impact. And this is, you know, traditional information technology, you've got there CIA Triad confidentiality, integrity and availability and often you want some -- want to flip the triad in a safety world and have it be availability, integrity and confidentiality, so the way you waive things is going to be different.

Availability of devices is important though, I guess this is a Steve quote, you know, "You can't reboot a patient," and clinical environment is very widely, you know, you've seen one hospital, you've seen one hospital and so how do you assess the impact in a specific environment?

So just to make this a little concrete, a couple years ago there was a published vulnerability in the Hospira PCA Infusion Pump. It was scored as a -- using CBSS as a 10 which is the highest and the vulnerability was remote Telnet route access without a password, but you can't just stop at the technical vulnerability you have to consider the health care impact, you know, what could you do when you exploited that vulnerability you could change the drug libraries, it wasn't clear whether you could actually change the actual dosages. There may be defense in-depth designed into the system, you know, if a human has to manually confirm the dosage change even if the dosage could be changed you've got a safeguard in place, a mitigation in place. You have to consider the environment. The pumps may be on separate networks that are trusted and hopefully, you know, well segmented and segregated. The vulnerable interface might not even be in use it might be turned off, I mean, we -- you know, you sometimes see cases where, you know, an interface is there, but it's not activated, so, you know, the vulnerability, you know, could potentially be exploited in some other version of the device, but maybe not in this particular one.

And so the implications are, you know, in your -- if you're in a hospital performing due diligence and, you know, managing the device appropriately that CBSS score of 10 is misleading. You might really have a minimal risk.

So when we think about scoring vulnerabilities in a health care setting, you know, there's some desirable features, you know, basically, you'd like it to be usable, not too complicated. It should be accepted by diverse stakeholders including manufacturers, hospitals, security researchers, patients, regulators and others. It needs to be flexible for taking into account different kinds of clinical environments, different kinds of device classes, you know, and different device classes in different environments. You want it to be repeatable. You want it to be validated and, you know, getting back to the slide I started with, you really want it to provide a common language to focus the discussion, help smooth, well, you may not get rid of disagreements, but at least it gives you a common language for talking about those disagreements and trying to come to some common ground. And now I will turn it over to Steve.

STEVE CHRISTEY COLEY: So given the different can I understand of requirements or preferences that way laid out for a good scoring method, last year we examined a number of different method and we so to speak settled on CVSS and for those who aren't familiar with it, it's something that's been long established within the enterprise IT space. It's how many organizations prioritize vulnerabilities that they need to fix. It's a well-established standard which has global support.

The structure of CVSS is broken down into three different components. The ultimate goal is to calculate a score for a particular vulnerability which will yield you a value between 0 and 10. And you do this by looking at different aspects of the vulnerability. The base component of the CVSS vector touches on fundamental aspects of the vulnerability that simply don't necessarily change over time. How much authentication is required in order to even reach it in the first place, for example? Then there's a notion of a temporal metric group. This is -- these are aspects that could potentially change over time that might then further adjust the score such as a vulnerability might first be announced, but there isn't necessarily proof or function exploit code that's out there and widely available, but once that happens, you know, the contribution to the CVSS score would be higher as opposed to whether if it's perhaps just a theoretical vulnerability or not necessarily fully understood.

And then another critical piece for how CVSS is laid out is the environmental group and this really takes, this is built into CVSS to try and allow individual organizations to interpret or reinterpret certain aspects of a vulnerability within their own environment. And as Penny already said, you know, if you've seen one hospital you've only seen one hospital. And so this is one place where we anticipate being able to support various environments.

Now, the latest version of CVSS is version 3 which came out, I think a couple years ago. CVSS version 2 had the widest adoption, but people have started looking at version 3 much more and that's been an emphasis of the work that Penny and I have been doing.

Different kinds of considerations here that are relatively new that do have certain kinds of benefits within a health care setting. One of them, for example, is the notion of using the environmental portion to potentially adjust how important confidentiality, integrity or availability are to you. And while this was slightly available in CVSS version 2, in version 3 this is much more important. It has a more significant impact on the resulting CVSS score. So this gives a lot more flexibility to hospitals to otherwise adjust a score that might look artificially high.

There are other aspects such as the amount of user interaction that is needed for an attacker to even be able to exploit the vulnerability as well as certain modifications to one of the most common ones the notion of attack factor, do you reach across a network or does someone have to be locally logged onto the system. There is now in version 3 a consideration for having to have physical access to the device.

So in utilizing CVSS version 3 and looking at it our anticipation, our hope is that we would not, we would be able to use it as is without potentially making any changes in that as we have continued to progress we don't anticipate at this point necessarily wanting to make or suggest any changes. However, what we've settled on at this point as an approach is to develop a rubric, a way of sort of asking a number of different questions written in health care, clinical specific kinds of language which then help the individual person conducting the scoring to then fill out the individual technical components of the CVSS vector. I forget the exact number, but there's about 15 different data points that go into the ultimate score that gets produced.

And we want to utilize relevant examples from health care H. We want to utilize language that is familiar to practitioners within that domain. And so this is where we are now at this point is we are in active development of a rubric such as this. So you can see on right-hand side here a little bit about some of the language one might use to better be able to interrupt and get a little bit closer to linking the technical impact of a vulnerability to what the health care impact is. So, go ahead. You can finish.

PENNY CHASE: So I'll take -- so what we've done is we've set up a cross stakeholder working group. There are medical device manufacturers, some health care delivery organizations, some cybersecurity researchers and some of you folks are in this room. We've also invited the First and Steve didn't mention it, but First is the organization that manages CVSS, it's the form of incident response security teams and so we've got a couple member s of their CVSS special interest group participating as well. They actually were really interested in our doing this, because this is really the first -- we were the first domain, vertical domain to come to them and say, you know people have some issues, some challenges with applying, you know, CVSS as is, you know, you've got a rubric, a scoring rubric there, but it's just generic IT and people don't alms know how to translate that into these other vertical domains, so they're actually really interested in having, you know, working with us and having us do this.

We work through telecons. We've set up a LISTSERV we have a collaboration group that MITRE manages on your DMZ to provide a place where we can keep our interim artifacts and other documents that members of the group are sharing with each other. We reviewed how some manufacturers and health care organizations that currently use CVSS, excuse me, how they use it and, you know, after we sort of had these meetings and these kind of discussions with user of CVSS came to consensus on the approach. As Steve said that we want to build a rubric that will provide guidance and develop examples of using the rubric and there may be actually multiple rubrics for, you know, for different use cases.

So now we are starting to develop the rubric. We decided to break into groups that would, one focusing on the base score, the other focusing on the environment score. Then we'll get feedback from the broader stakeholder community and our ultimate goal is to put together a medical device tool qualification package. So an MDDT is a tool, it's a program that FDA has initiated and the idea is if there are useful tools to provide evidence for making regulatory decisions, you should be able to go and have this tool, have it validated that, you know, it provides appropriate evidence and then FDA is not going to have to ask a manufacturer to go and provide them with the evidence that this tool operates the way it does, you know, that this has been once and so the hope is our goal is at the end of this we will put together a qualification package.

So I'd like to extend an invitation if there are people in the room or on the Webinar, you might be interested in participating, you know, potentially even be on one of the two subgroups or being part of the community that we will then send, and, you know, ask for feedback, please see Steve or me sometime during the sessions and we'll get you hooked up.

DINESH PATWARDHAN: We have time for one

question. We want to stick to the schedule. There's no burning questions? Next time to --

STEVE CHRISTEY COLEY: I really hope there is a question. I need some time to do this. Someone better ask something.

UNIDENTIFIED SPEAKER: I've got a quick question, so I'm just curious, so in having flexibility in the rubric that to me means that you let judgment play a role, right, and obviously how people are scoring things. How do you address the issue of bias? So I will be inherently biased to score my own vulnerabilities lower than maybe a third parties, so what, can you guys address how are we trying to tackle that issue in this?

STEVE CHRISTEY COLEY: Bias is definitely a challenge and it's historically been a challenge within CVSS even though CVSS has as a goal consistent evaluation. If we can structure the rubric properly and ask appropriately -- sufficiently detailed questions that might take away at least some of the bias, but one of the big benefits of a scoring system such as CVSS is that not only do you get a score at the end of it you have a detailed record almost of all the different decision points that were made and then potentially when there are disagreements that at least helps to focus the area where there may be disagreements.

PENNY CHASE: Just to reiterate on that the, you know, a fundamental piece of this is to facilitate communication, you know, sometimes people just look at the score and folks say, you know, you really have to look at the vector and, you know, maybe people don't, but they should. And our feeling is that if we've got this rubric which records, you know, rationale for making certain decisions in filling out the elements of the vector that comes along as part of the CVSS process and that's what could really help, you know, say a hospital interpret the way a manufacturer scored the vulnerability.

UNIDENTIFIED SPEAKER: How does one capture if a vulnerability is being exploited in the wild and how does that affect the CVSS score?

STEVE CHRISTEY COLEY: So I don't remember every single individual detail within CVSS version 3, but I don't think it actually accounts for in the wild exploitation. However, there is a little bit of flexibility where we could potentially take advantage of it within a rubric. There is some flexibility within the environmental score to significantly raise the importance of certain aspects of confidentiality, integrity availability. So there may be some mechanisms there, but it's not a clean mechanism. It is a question that is not asked within CVSS. That said we don't anticipate CVSS scoring itself to be the be-all and end-all of how organizations do risk assessment.

So whether it shows up in the rubric or as a series of additional questions I would expect that certainly something such as in the wild exploitation would become a factor in there and we would at least want to record it.

UNIDENTIFIED SPEAKER: I'll just remind you one of the fields actually states whether or not the exploit is theoretical or exists in the field proven, unproven.

STEVE CHRISTEY COLEY: Yeah. Just the existence of an exploit doesn't necessarily mean that there is widespread exploitation, however. One of the -- for those who aren't familiar with vulnerability research, researchers may find things, but not necessarily know what they've found or the extent of how significant the problem is. They might just find indications that there is a problem, but not necessarily be able to figure out what the severity is.

There's a period of research even for an individual vulnerability before there's a complete understanding of how bad it is.

PENNY CHASE: With that said we could leverage the temporal score and, you know, perhaps in the rubric, you know, indicate that you might want to use one of the values to indicate that there are exploits in the wild, so.

DINESH PATWARDHAN: Let's thank our speakers.

STEVE CHRISTEY COLEY: Thank you.

DINESH PATWARDHAN: We are going to change gears just a little bit. Next up is Kevin McDonald. Kevin is the Director of Clinical Information Security at Mayo Clinic. The title of his talk is How Medical Devices Diversity and Uniqueness Drives Its Challenges.

HOW MEDICAL DEVICES DIVERSITY AND UNIQUENESS DRIVES CHALLENGES

KEVIN MCDONALD: Thank you. So after a healthy dose of Macallan single malt scotch I decided to change my presentation title to Buried Under an Avalanche, a Medical Device Special Snowflakes.

We'll talk later. So a little bit about diversity and uniqueness. We all realize in our fields that bracing diversity and uniqueness is great in people, cultures, lifestyle, new ideas, opportunities, I have people on my team from Greece, from Brazil, multiple countries, Nigeria, Kenya and it's wonderful.

On the other hand diversity and uniqueness in medical devices actually has a detrimental effect. You can end up decreasing security and safety, increasing your chance of errors, workload goes up, resources needs goes up, cost goes up and it actually impact s your patient care processes.

So if you're a big believer in things like Six Sigma or human factors you realize that, you know, variation really is undesirable, because you really can't be certain what your ability to produce a desired outcome. For any of those of you in hospitals who've ever decided to scan your network, you now know about the ability to produce a desired outcome with medical devices. And when you have special cause variation the system really isn't stable or predictable and in human factors again that also the more complexity there is the harder it is and you should really try to simplify and streamline.

So a little bit our environment. We've got about 25,000 currently networked devices. I can tell you that I know I have 5,000 unique devices based upon vendor, type, model and version, but I know it's more because we don't track down to patch level. We don't track down to, you know, what version of Linix it is who's the distro on that, et cetera.

And our devices can be as simple as cameras or as complex as our proton beam therapy equipment which there's like I think 10, 12 of them in the United States right now. And a lot of these also require a family of other devices to work, so they're hooked to something which hooks to something which goes onto another thing which then has a direct pipe to hopefully not the UK.

So a couple assumptions we need to make and I -- these should not be new to anybody in here. All networks are inherently insecure. You need to have multiple layers as a defense as you go from the outside from the border in. That even includes down to the individual devices. That's sort of your last ditch effort to be able to stop things. And the greatest security impacts, of course, really are not and while I, you know, we need to continue our research on all of the new things that we can do to protect devices, quite frankly, I have a boatload including a big anchor of legacy devices and until manufacturers start turning things out designed securely I have to deal with today's practical issues.

So we're looking at simple things like have a good inventory of your devices and your software patching limiting, you know, the software can't be run, white listing or antivirus, restricting administrative privileges, no default hard coding or non-expired passwords. Just very simple stuff that actually make a huge difference. You can take 60, 70% of your risk off the table just by doing those simple things. So you can tell we're a big fan of the critical security controls and the Australian signal directorate, so.

Other assumptions that we have to make is that health care institutions don't have the time, money or the resources to just independently take care of these and from our point of view cost and effort for security in devices should not and cannot be the full responsibility of hospitals. It's been a while since I've heard, well, you need to put on a secure network, but it still occasionally pops up once in a while talking to vendors.

Just to emphasize that, a little bit of health care demographics, 24% of hospitals in the United States are critical access hospitals, that means Medicare has to pay them more just to stay open. About 1,700 have less than 50 beds and 4,000 out of that 5,564 have less than 200 beds. Mayo Clinic is not the real world. Take my word for it. Mayo Clinic is not the real world. Those people really have difficulty when you start talking about medical devices. You look at the finances again, they rate finance COs write finances and the number one issue NOI is about 2.6% right now. There's about 670 real hospitals that are vulnerable to closer. Significant issue. Those are the people we need to keep in mind, not Mayo Clinic. My budget for medical devices exceeds a large majority of the NOI for rural hospitals.

Health care also only started investing in security within the last five years and it's rare to have a security organization, smaller organizations have no dedicated security researchers.

So a little built of the special snowflake. You can read all of those different things that we see or variations, operating systems all the way down to security aspects. Operating systems, we still have some stuff with DOS. We were -- we did a pen test on it one time and we wanted to load Pong on it. Our problem was finding an old enough version of Pong.

UNIDENTIFIED SPEAKER: No Windows 3.1?

KEVIN MCDONALD: No. Not that I know of, but it could be there. NT, Vista, every other flavor, throw in proprietary, embedded, various real-time, all sorts of different servers, Linix, Unix and some of this stuff unknown and if you take the next step below that we can have various different patch levels, updates or release levels on each of those.

Software maintenance variations, again, it's kind of one giant grid, sometimes you can do operating system updates, sometimes the vendor will test to see what causes problems and only give you the things that don't cause problems. You can get full updates some are just no updates at all. The application software, you have multiple variables there. Other commercial off-the-shelf stuff, full, select, no and again, you got to realize that each one of these can fit in with another one below if for each device, so that 7,000 unique devices based on vendor, make, model can actually continually be, each one can be unique themselves, based upon all of these attributes.

Third party open source timeframes for when maintenance can be done. Some are monthly, some are 60 days, some are annually, some are a combination of all of the above for some of the software, but not some of the other software. Who it's performed by sometimes the health care delivery organization does it, sometimes the vendor does it, sometimes the third -- a third-party contract does it, sometimes the vendor will do the application, the hospital will do the software. It again, some of the processes you can do it centralized, some of them sneaker net. We still have some stuff which requires a lap top and a serial cable for somebody to go visit each of the devices. And to have the patient out of the room during that time.

Other system variations. Maintenance tools. You can do everything from using our standard Tivoli big fix to proprietary to sticking in, you know, USB ports, connection methods, multiple different wireless. You can have it wired. Authentication methods, again, you can have active directory, LDAP, they can do it internally. Encryption, you can have multiple variations there. External vendor access. This is becoming much, much more of a problem. They have multiple tools. I can tell you we got SecureLink. We've got Bomgar. We've got vendor rebrand ed of those. I -- and there's probably even somebody every once in a while firing up going to My PC that I haven't found yet.

Configurations, there's a wide variety of what ports are open. What active services are. Some places actually still use things like, you know, trivial FTP and Telnet to be able to do some of their work on a -- security variations, antivirus that can be anywhere from none to their proprietary brand to they let us manage it and we manage it like any other Windows servers too. They let us manage it, but we have to exclude certain folders. Different update schedules. They can have white listing or not which, by the way, is one of our holy grails not antivirus, white listing.

Security agents. Sometimes we can put them on. Sometimes we can't. Sometimes we're vendor approved. Sometimes we do it anyway. Scanning also known as DOSing yourself. More likely at all you're unable to. Sometimes you can just do a discovery scan unauthenticated or every once in a while you find something you do an authenticated scan on which again is another one of our holy grails. I can go through all of the firewall variables, but you're -- I could go on and on and on, but you get it by now.

So the impacts of this are there's just a dizzying array of uniqueness and variation. And with that it's really hard to get to an acceptable level of risks. There's a huge pluraflation [ph] of tools and solutions. You've got a multiple set of tools to do maintenance. You've got multiple sets of antivirus running. You need to handcraft individual solutions for each of these. Which means you now have to have a huge technology knowledge base. You've got to have somebody who remembers how to secure which is sort of an oxymoron DOS.

Airpro [ph] and manual processes, when you when you handcraft those bad things happen. People put in the wrong IP address and shut down your radiology department. And you're really unable to scale those solutions at -- for at least us, if you're a small hospital with one CT and one MRI you can scale it. Once you start getting into larger institutions you can't scale that to 50 MRIs, 50 CTs and the rest of the radiology equipment. And really being able to track this various combination manually is virtually impossible. And when you can't scan, our ability to be able to make sure that quality control is done that all of the things that are happen are supposed to happen, again, is extremely hard.

So some of our challenges, you really can never get secure enough. It costs a ton of money to be able to do this. When you start looking at handcrafted solutions, compensating controls. The interesting thing now is that medical devices now become the weakest link in your enterprise security devices.

Just recently, we pushed out everything, you know, there are a few things we were able to scan. We found that they were missing some patches. We for all of our IT managed stuff, we pushed those patches out. Those were looking pretty good, all of a sudden, our weakest link was now medical devices and our facility systems.

The number of peoples and skills are impossible to get. They just aren't there, particularly when you're at a small rural hospital where you can't may the salary and there's nothing to do, but throw dried cow chips on the weekends.

Your compensating controls again, become very unwieldly and they don't scale. You can't put a small little firewall in front of everything. The VA has 3,200 distinct LANs with ACLs, last I heard somebody maybe correct me, they have 60 people who run this and they can't and it's unwieldly. They just can't do it anymore.

Because of the fragility, you know, and the device issues you can't use any of the standard management techniques. So you can't do standardized patching. You can't do standardized vulnerability management. These are on the other end of the spectrum from your Windows servers and your data center and again, errors are made. Just because of that variability. And so what happens is if someone organizations just don't try or can't afford to even try to manage any of these.

So some of our observations and we are at a conference again, of the Milk and Global Conference the other day and somebody kept talking about well, can't somebody just develop a -- there is no killer app for this thing. There's no segmentation strategy. There's no firewall, there's no antivirus that will fix the problem. It has to be a combination of things. And sadly, for many legacy devices, there are no solutions other than segmentation or local physical firewalls. Until these things turn over many of these things we're still buying today, because they're the only thing available. And many of these devices the expensive ones have a life 12, 15, sometimes up to 20 years. They still work. They still provide adequate patient care and again, if you're -- have a 2.6% NOI you aren't going to be buying one every three or four years.

The smaller hospitals, physicians' offices are in big trouble. They just don't know it yet. And even if we wanted to and could afford to there are very few secure devices to buy. We could give you a handful that we've tested that we know are really secure. In interesting point we have also found now, is that some vendors are selling security as an add-on option. So if you pay a little bit of extra money we'll add on some of the white listing. We'll add on some things to be able to manage your authentication better, things like that. So it causes us problems because when they go and answer our questionnaires they do an MDS2. All of those things are available. When the bid goes through guess what gets left out? So the clinical areas don't want to pay for that and don't understand it. And health care workers are -- institutions are getting smarter, but they still have more work to do to pressure the market.

I love finding good quotes. A couple of my favor ones on here are, how can you govern a country which has 246 variety of cheeses, from Charles de Gaulle. I thought that was kind of appropriate. How do you manage medical devices? The last two are great. We haven't had to use that one again in a while where a vendor said we've never had one.

Of our devices compromised and so one of our staff said just because I've never been shot doesn't mean I'm bulletproof.

So that's the end of my presentation if there's any questions.

UNIDENTIFIED SPEAKER: Can you buy patient safety as an add-on?

KEVIN MCDONALD: No.

ATLIEN SCHMIDT: Atlien Schmidt [ph] from Deckert Research [ph]. When you say white listing I think you have a different definition than I do. Can you please give me your definition?

KEVIN MCDONALD: That is only allowing known services, applications to run on a device. Which for a medical device from a health care delivery organization sounds like it should be extremely simple, because medical devices have to be well tested. They have to be FDA approved. You should know exactly what is running on that device at all times.

ANDREW MCGRAW: Andrew McGraw with Integrated Clinical Solutions with the Army. One of the big issues that we have, one, we have vendors tell us that the commercial world doesn't want security, so they don't really want to play with us. So that's one of the --

KEVIN MCDONALD: We hear that too.

ANDREW MCGRAW: And then we have the DODCIO that yells at us and tells us that all -- that medical device are IT and have to be integrated in and we have to run all the rules and everything to have every -- we're just sitting there shaking our head and every single slide you had, but my question is, you know, we're running into an issue now where they're telling us we have to scan and we have to scan live devices and we have to scan according to their schedule and we had an issue with one of our CTs that got scanned with a patient on the table --

KEVIN MCDONALD: Oh, yeah.

ANDREW MCGRAW: -- and had the dye injected and the CT shut down. So how from your perspective are you trying to schedule scans or what are you -- are you trying to do just a baseline to say that this is what it's supposed to look like or how are you attacking that?

KEVIN MCDONALD: So we had a couple of really bad experiences. So quite honestly, we're not scanning any of the end point medical devices. We'll scan some of the computers that are associated with them, workstations at -- we're trying to figure out, we're going to do things, one is that we're working on a non-boarding process of where when we get any new device in we're going to hook it up and our threatened vulnerability management people are going to scan the crap out of it and find out if we spoke it.

The second thing that we're doing is we're really trying particularly for the legacy device, because some of them you just, you know, you just ping them and they fall over. And we're trying to find something that will allow us to be able to at least find them and do some monitoring on them in a passive fashion. I don't have a solution.

ANDREW MCGRAW: Like I said, we're in trouble because they're mandating that with that --

KEVIN MCDONALD: You're skewed.

ANDREW MCGRAW: -- it's supposed to be scanned and, thank you.

KEVIN MCDONALD: Yeah.

ANDREW MCGRAW: I really appreciate it.

KEVIN MCDONALD: If you needed validation, I'll -- when they fire you let me know, we'll -- we always got openings.

UNIDENTIFIED SPEAKER: Do you repeat the onboarding process when a major software release comes out for each device?

KEVIN MCDONALD: You know, it would be great. I don't think I have the resources to do that, but that's a good question.

UNIDENTIFIED SPEAKER: Ty [ph] being one of the bigger ones.

KEVIN MCDONALD: Yeah. Great question.

UNIDENTIFIED SPEAKER: Has anyone? You said you have the most probably some of the largest resources.

KEVIN MCDONALD: I can't imagine. I have 13 people in total who do nothing but medical device security and we partner with our HTM and they're up over 100 people right now and growing larger everyday. So I have more resources for medical device security than the vast majority of institutions have for just security.

MARK POTTER: Mark Potter from New Wave. Thanks for your presentation. One of the questions that I had was whether or not the Mayo Clinic has in its asset management system does it have something that ties in essentially whether a medical device is in use bedside or whether it's essentially available for patching and is that tied into your patch management.

KEVIN MCDONALD: We don't have anything on whether it's currently in use or not. We've got a fairly robust, depends on when you talk to. They are BioMed people. Use some inventory workflow tools. We find that extreme ly valuable, because they're able to capture IP addresses, they're able to capture a bunch of basic demographics about the machine. One of the things that they also capture in there though is some joint commission scoring and by using that joint commission scoring we found that extremely valuable, because it tells us where it's used, what kind of functionality it has, whether it's life dependent or just strictly diagnostic and so we're building that. We've already built that into our incident response, so, you know, part of our incident response, you know, is if it's, you know, really bad and has potential for patient care we aren't going to knock it off the network and --

DINESH PATWARDHAN: If there are no more questions let's thank our speaker.

Our next speaker is Rob Suarez. We are going to change gear one more time. He's the Director of Product Security at Becton Dickinson. The title of his talk is Building Cybersecurity Programs for Healthcare Technology: Our Only Security is our Ability to Change. Building.

CYBERSECURITY PROGRAMS FOR HEALTHCARE TECHNOLOGY: OUR ONLY SECURITY IS OUR ABILITY TO CHANGE

ROB SUAREZ: Thank you. Hi everyone. My name is Rob Suarez as Dinesh mentioned I'm the Director of Product Security at BD. BD is a global medical technology company and do I have slides? Oh, I do. Break time, coffee. No. Well, I've got a USB stick that I could give you.

DINESH PATWARDHAN: Yes, please. He's doing it.

ROB SUAREZ: He's got it on e-mail, yeah.

DINESH PATWARDHAN: We have a secure USB stick that's coming through, so just 30 more seconds.

ROB SUAREZ: I saw that. Yeah also had like a nine character password though on his iron key. Oh, it's Dinesh's fault, okay. No. The slides aren't that good anyways.

UNIDENTIFIED SPEAKER: If you read the labeling it did say the scan will continue in the background even if you dismiss this dialogue. This is -- there's a very strange --

ROB SUAREZ: I have it, it's just not -- all right. Hey, you know, maybe we'll just do it live. We'll do it live. All right, guys, it wouldn't be the first time.

So let's start over again. My name's Rob Suarez I'm the Director of Product Security at BD. BD is a global medical technology company. We sell a wide variety of products from infusion pumps to lab automation systems and syringes and other types of medical supplies. And the folks at the FDA have asked me to share with all of you today my journey, my experiences in building a product security program at a medical device company. And it's not to say that it's by any measure perfect or that we've reached some destination. I truly think this is a journey and it is about continuous improvement. If there's one thing that you get out of this presentation today it's that this problem is evolving and the way that we treat it should evolve as well over time and that the way we look at security should fundamentally change.

You know, the first thing I would say that you would want to do in building a security program is to establish a mission, vision and values. Notice I didn't first say risk management; right. Or do a risk assessment. You know, risk assessment's really important. It's important to do risk management traditional risk management. And I think most major corporations, most companies are -- that are successful are good at doing risk management. What's challenging is in security when we're just focusing on risk where do you go. Where do you go and where do you end?

And so at BD just to give you an example we like to say that in product security we strive for security by design in use and through partnership. And so we can do all that we can to building good security controlling into our products, but ultimately, our products reside in any given environment. Perhaps a hostile environment and ultimately that product has to be used by someone else, someone that did not develop that product and from a security perspective, you know, someone else needs to manage the security of that product; right.

And so how do we consider the user's experience, the customer's experience when they're procuring and using and decommissioning a medical device? The partnership aspect is that we try to engage our customers, not just the clinical user, but the IT folks that have to manage connectivity for these systems and the security research community as well who provides us with a different perspective on security for these products. And also our standards bodies and regulatory agencies like the FDA, like the Department of Homeland Security. They are partners with us. Oh, thank you. So now this will all make sense.

Yeah, they are, oh, come on, R&T, there we go. They're partners with us in this journey and when you're building your security program you need to leverage those partners for different perspectives. It's one thing for me to go around in BD and tell everyone you need to do security. It's another thing when I have the Mayo Clinic say, we need to do security or the FDA saying device manufacturers, you need to address security; right.

Those -- so security by design in use and through partnership is certainly a kind of a mission statement for us. It's what, you know, my team wakes up in the morning and, you know, focuses on in their day-to-day activities, but I also say that we strive to achieve transparency with our customers, that means, you know, how do you secure something that or how do you secure a risk that you know nothing about; right. And so providing our customers with communication on security risk, you know, not being afraid to talk about vulnerabilities. Every product, every piece of software out there has bugs. Vulnerabilities are a fact of life. And a security program is not about 100% security, it's about establishing a mechanism to continuously address vulnerabilities, address security risks as they come up. You know, establishing that up front I think helps eliminate the fear in talking about security, right. We're not, you know, talking to R&D folks and calling their babies ugly; right. We're trying to help and we're focused on a mission and vision and values.

We also, another principle at BD is offering customers control, you know, if we sell a product that's running windows then we like to offer our customers control over that Windows product. Are we 100% there yet? No. No, we're not, but this is a journey and this is our mission and vision. This is one of our principles is offering customers flexibility to do things like active directory integration, you know. To leverage a customer's antivirus solution, because you know what's worse, what's worse than no antivirus solution? It's having an antivirus solution that just never gets updated. It's pointless. It's pointless and we can't get every customer to agree on what is security. I mean, we can't get, you know, one customer, two customers to agree on what a complex password is, right. This is why we make it a principal to offer our customers control over security. Otherwise, it's just too difficult to wrap our heads around, you know, what we want to give our customers from a security perspective, offering them control and that makes it a little bit more scalable, because your customers might be large hospitals, they might be small labs, right. And so you want to offer, you know, a product that considers security and that is scalable to those different customer bases, but -- here we go.

This is the juicy part. You know, you're about to start your journey in rolling out a product security program you're going to need strong leadership support. Okay. You could do it without leadership support. You could try to, but it really helps to have your company's leadership understanding what you're asking for.

I usually talk about my mission and vision with leadership. And I talk about risk reduction as well, but I really talk about, hey, you know, you want to sell a quality product, how can it be a quality product if it's not secure? And then you're going to turn around and talk to you engineering teams. And you're going to need help and the tough part is that there's not enough security professionals out there to hire and you can't hire enough; right. And this is why, you know, in my journey I've focused on building a community of practice.

I've got a team of people in a product security organization, however, product security does not happen in the product security office. It happens with the R&D folks, the service engineers, the marketing and communications teams are legal and regulatory affairs and quality organizations participating and contributing to our purpose.

And this is the framework, by the way, that we use at BD and you'll get the slides after the presentation so you can take a look at this. I think what's to note is that we're asking a lot from our organization, so being clear in what we expect is so important to simplify this and this is the foundational stuff, okay. This is the -- these are the security activities that we incorporate throughout a product life cycle, not just the development life cycle, but the product life cycle. And then we build off of that continuously.

So next year my team is not going to be doing the same things that they did last year. Maybe we're not going to do, you know, risk assessment next year. Maybe we'll train our quality organization how to do a product security risk assessment. Maybe next year we're not going to do static code analysis and vulnerability scanning, maybe next year we'll train our R&D organization how to do static code analysis and vulnerability scanning. And next year we'll find new things to do, new challenges to take on.

We've, you know, we've -- I've also had to think about how to delicately insert security into a product life cycle, it's a lot that we're asking for, but finding the cross sections between what a manufacturer is doing today and security activities has been very helpful. You know, for example, device manufactures do risk assessments all the time. And they're very quality centric. You know, what if you train those quality engineers how to look at security, how to do a security assessment, how to leverage the common vulnerability scoring system, incorporate that into your risk assessment. You can establish design security requirements, incorporate that into your design input.

You -- there's elements of the security program that you have to simplify as much as possible and one thing I strongly recommend is having clear and source from authoritative sources, secure coding standards and hardening standards. So, you know, if you're familiar with SCI Cert they have a very good collection of secure coding standards for multiple languages. If you're familiar with the DOD, the DOD has done a remarkable job of developing DISA, STIGS [ph] and DISA as well, by the way. Developing STIGS those are Security Technical Implementation Guides. You don't need to reinvent the wheel. Those things have already been done. If you want to know how to harden and secure a Windows operating system someone has already documented that for you. Don't let your development teams struggle on those types of issues and worse, don't just do a risk assessment, don't just do penetrating testing or hire security firm XYZ to go do penetration testing and find vulnerabilities and call it a day. No. You have to establish up front what are the right things to do during a development process. And that's why, you know, I like to emphasize design requirements for security. Hardening standards and secure coding standards as well as identifying where your regional and marketing requirements for security and start patching in development phases. Why? Because it's like training a horse, you know, you don't just show up at the race and, you know, tell a horse to start running, no, you got to train and patch management is just like that as well during development figure out how you're going to maintain patches.

Vulnerability scanning and static code analysis is not just about finding vulnerabilities. If you have those up front requirements for secure coding and hardening standards, right, it's about finding out in your process what went wrong. Where did you miss out on a secure coding standard? How did you leave that hardening standard, you know, out of your operating system image configuration.

Finally, you know, if in the development phase, you know, if you can address those kind of fundamental aspects it makes penetration testing a lot more interesting. You're not just finding missing patches. You're not just finding, you know, a hard-coded password or brute forcing a password field, you know. No, I can turn around and ask my software developer if they, you know, did you put any password restrictions? You know, what's the character limitation on that password field? I don't need to brute force a password field during penetration testing, you know, not in product security. You know, this is why I, again, I go back to building a community of practice and those individuals across multiple functions to help you build out your product security program. You're not going to have enough people. You got to get R&D, service and a whole bunch of other functions involved.

Lastly, and I'm going to and, by the way, you can see in this kind of visual some of these activities map to typical quality management system. You'll see at the bottom there design control complaint handling of risk management. Yeah, I mentioned, simplifying as much as possible and if you have design requirements for security, you know, there's plenty of authoritative sources to pull from in doing that. And also, you know, I strongly recommend having a very formalized risk assessment process. Not one that replaces, you know, FMEA, right, or hazard analysis, right. I'm talking about just something that's security centric. You still want to have, you know, those traditional quality risk assessments. You still want to have those. You're going to have to get out of your chair and walk over to the quality organization and ask them, hey, can I have you sit into this security risk assessment? I think might want to follow up with a hazard analysis.

There's no one singular form of risk assessment that solves it all. There's -- not right now, you know, maybe we'll have a research study after this to figure that out, but right now you have very good practices in terms of quality to do those types of assessments and the security engineer is not a clinical engineer is not a doctor. And so again, you're going to have to have these multiple disciplines at the table to do a risk assessment.

Train up your existing organizations. So them what you're asking for. Show how it applies to their roles and functions and get them involved. You know, when you're drafting a communication about security you're going to need a lot of people to understand what you're talking about. You're going to need the R&D folks to be able to perform a risk assessment in the security context. You're going to need them also to understand the importance of patch validation, right, or validation of a security control to remediate that vulnerability. You're going to need service folks to understand the importance of deploying these patches. You're going to have to have a plan established ahead of time before an incident, before a vulnerability. How are you going to roll out that fix? And you're going to even need the marketing and communication person to not fear a security bulletin, right, to talk about these uncomfortable things publicly and you're going to need them to understand that in a very timely fashion, because when there's a security incident you need that immediate buy in you need to look past that, now we need to find out what information is actionable to customers in this security communication, right.

And so this is my last slide, here. I go back to transparency and collaboration. You know, to give you an example at BD, we are in the process of drafting these product security white papers. If you've seen an MDS2 form, it's a piece of security documentation that walks through the risk and considerations for this product. It goes a little bit beyond the MDS2 form where we're really showing also data flow diagrams, process diagrams as well, a listing of third-party components in our product calling out the sensitive information that rests in transit.

Offering your customers that level of transparency makes your life a lot easier. Because you're enabling your customers to take action on these risks and you'll see at the bottom there, private security notification, you know, when you identify a vulnerability, when you have a third party report vulnerabilities to you, you know, leverage that as an opportunity to really understand which way is north that, you know, a vulnerability disclosure is a means of our -- for our customers to address risks that were perhaps were unforeseen by the manufacturer, but your product security white paper is also a form, a means for a device manufacturer to communicate security risks to the customers; right. You separate the two. You know the risk that you have today, communicate that to customers. You might have risks that you don't know about that might get reported to you, right. And again, transparency I think in both of those aspects are very helpful. And especially in building your security program which can be challenging. So with that I'll open up for questions. Are we okay on time?

DINESH PATWARDHAN: Yes, we have time.

UNIDENTIFIED SPEAKER: My compliments on a lovely talk. I -- as a human factors we need, what I notice is a common theme that you are pushing the security to the locust of control where it actually resides through the executive suite, R&D, to your customers and to your service and marketing people and I think that's a brilliant way to handle it.

ROB SUAREZ: Thank you.

JEREMY EPSTEIN: Great talk. Jeremy Epstein, National Science Foundation. I want to take a slightly different angle. You're presumably hiring computer scientists, biomedical engineers.

ROB SUAREZ: Great question. I wanted to --

JEREMY EPSTEIN: So --

ROB SUAREZ: I wanted to tell you guys about this.

JEREMY EPSTEIN: Okay. Can I ask my question and --

ROB SUAREZ: Go ahead. Ask your question. Sorry.

JEREMY EPSTEIN: What skills do they not have or do they have and how should that -- how should we be changing the curriculum or do we need to change the curriculum so that when you hire them they actual ly don't create you these problems that you then need to fix?

ROB SUAREZ: Yeah. Yeah. Great --

JEREMY EPSTEIN: I don't know, maybe that was a different question than you were going to -- or answer, but.

ROB SUAREZ: No, it's okay. I'll take it as two questions. Am I hiring computer science majors and b) what do we need to change in their curriculum?

Okay. So here's the deal, guys. You know, I've hired some pretty technical smart people who know software engineering, but also know systems engineering, who know general IT and the various disciplines within technology are really important to get into your security program, because they give you different perspectives. I'll add on to that.

I also hire completely nontechnical people. One of the folks that I have on my team who does -- facilitates our vulnerability disclosure process, she is not a technical person. She's actually -- she has a journalism background, but she does an excellent job communicating to customers about security and distilling it in a very easily interpretable way.

We have technical people to help her, you know, explain, you know, the 1s and 0s, but, we need also someone to extrapolate that in a higher form at. We also have also a program manager who's a -- who is formerly a product manager, nontechnical, but me knows the development process. He knows the process to get a product commercialized. And so when we're drafting our policy and procedure it's really important to get that feedback, that pushback. And how do we address this in our curriculum today? I'd say that, oh boy, it's been a while since I was in college, but in, you know, grad school, I remember actually there was no program for security and I think when folks are learning how to program, if they can learn very good design patterns and then security design patterns and then secure coding practices, for example, as a software engineer I think that's very important. Even understanding the authoritative sources to go to. And like secure -- hardening standards as well, just knowing where to go to, because they're going to change very rapidly, but in appreciation for what can happen in a -- at a technical level when they're learning how to program.

JEREMY EPSTEIN: Can I ask a follow up? So in addition to the problems that are caused by computer scientists if you will, because their software has vulnerabilities and -- are there also problems, security problems that are caused by the mechanical engineers, the biomedical engineers et cetera, some of these other specialty areas who are not computer scientists, who are not security people, but they do things that end up causing security problems and therefore they -- had they had some security training you might have been better off, but security training isn't part of their curriculum?

ROB SUAREZ: That's a great question. You know, I would say -- I've observed, certainly in a physical security where I think other disciplines can use some security education. A great example is, you know, physically securing sensitive information at rest even when, you know, it's stored encrypted, right. You know, you can still have, you know, a great example recently is like, you know, we had an advisory that talked about passwords stored on compact flash memory, right. And, you know, understanding how, you know, you can bypass the, you know, the software level encryption and via hardware, you know, extrapolate that information is important to at least to understand in a general concept, yeah.

GEORGE SAMARAS: George Samaras. I believe the classic example for his answer for his question is the electrical and mechanical engineers that install the USB port.

ROB SUAREZ: Yeah.

GEORGE SAMARAS: So the doctors can charge their iPhones while they're treating their patient.

ROB SUAREZ: Yep. Or JTAG ports, you know. Yep. Great.

TIM BECK: Tim Beck with Roche. Just quickly, first, great presentation. I like it, it's coherent and together. As far as putting notifications out to the field it sounds like you've got that handled. Do you have actually a process for taking notifications in from the field where it gets correctly routed as to whether once researchers point of view or it's a black hat attack or do you have anything --

ROB SUAREZ: Oh, good question. Yeah, it's a little bit more -- it's a little bit more challenging. I think it goes back to actually building the community at practice. If you can incorporate in your complaint handling processes across your organization a bucket for security issues and events I'd rather have all of our service folks on the front line, familiar with how to route a security issue rather than having a back office group of, you know, five people, you know, manning the phone and looking at e-mails, yeah.

DINESH PATWARDHAN: If there are no further questions. Let's thank you our speaker for a very good presentation.

ROB SUAREZ: Thank you.

DINESH PATWARDHAN: Our next speaker is Todd Carpenter. Todd Carpenter is the Chief Engineer and Co-owner of Adventium Labs. The title of his presentation is Even in Theory, Getting Medical Device Security Right is Difficult.

EVEN IN THEORY, GETTING MEDICAL DEVICE SECURITY RIGHT IS DIFFICULT

TODD CARPENTER: Thank you, thrilled to be here. The concept for the title in theory, theory is the same as practice, but not really in practice. I'd like to say in theory security is solvable and in practice, we just haven't done it right, but this workshop is about gaps and there's many, many gaps in security, many areas that we need to improve what we know and techniques that we have to solve in there.

Motivation for this, there's a great cartoon, ex case ed [ph] if you don't follow if, it's worth following. I just at least one professor that uses it to help teach security and I'll read it for the people in the back who can't read it.

"Our field," so this is chief engineer for a medical device company talking about product. "Our field's been struggling with this problem for years. Consultant comes in, struggle no more, I'm here to solve security problems with algorithms. Or a substitute, snake oil, encryption, checklists, whatever."

So consultant works and the team works for a while and six months later, wow, this is really hard. Security is hard. You don't say. So popular attitude seems to be that security and doing it right even for medical devices is like falling off a log and I'm an engineer, I can tell you it's really easy to fall off a log, but it's a little harder to get the security done right. And there are a lot of threats out there and it's not getting any better.

A few years ago the biggest threats were really in the breach, the privacy, the attacking it to get the information out and they figured out how to monetize the health care records, but what's really scary is they have figured out how to monetize the attacks directly. We're seeing that with ransomware right now, obviously. And we're also seeing that with companies selling short and attacking companies directly to make money out there.

We're also seeing security companies that are providing services for hospitals attacking those hospitals, exposing their live information to increase their own sales. So it's a scary environment that we're in right now and it's not getting any better. There's no sign that the attacks are going to get nicer with time going forward. And there's a lot of need out there in that industry.

We're particularly interested in the small medical device companies. We have a lot of the large medical device companies that are present here in this meeting, but 80% of the companies out there have 50 or fewer people. The median is actually much lower than that. What's the chance that these companies have an actual real live product safety is security expert on staff? Good luck, there aren't that many of those people out there in industry. It's pretty carry out there and we know the large medical device companies are always had challenges. So we still need solutions out there that all these organizations can use.

So Dan talked about this earlier. We're working with DHS right now and we're developing a platform for basically an integrated safe and secure platform that these small companies can use to start their development out there. And the concept is we're working with where we can commodity hardware. We're looking at different architectures, different ISAs, both remembered Intel. Putting a separation layer on top of that. We're using different separation layers that are available. We haven't developed these ourselves. We're leveraging work from DOD, DHS, other organizations and the separation layer that's one of the core concepts of good security is you keep things separate.

Now earlier, Kevin talked about the issues of port scanning. There's been some interesting cases where large medical HDOs, they've gone and port scanned so they figure out what's actually on their network and the device falls over. That's not good behavior. You want to separate that networking behavior from your safety functionality so that if something like a port scan does happen so that those IT people can actually do their job you can guarantee that the device isn't going to fall over that your safety functions are still maintained.

So separation, it's one of those core concepts. And earlier we had a question can you do security that has other pull through benefits to make it worthwhile? And we go into organizations and if we're just adding security it's a hard sell, because security is a cost often perceived incorrectly without direct value to it. But with things like a separation architecture we're also providing model A system engineering tools and determinism, non-bypass ability with this basic architecture and we're working with academia to bring in new innovations and get it out there. When you put all this together you actually end up with a development environment and a more deterministic timed to product. And we did this decades ago. We did this in avionics, so Adventium, we fit, we worked with multiple customer funding organizations, we're not a product organization, we're R&D. We work with NASA, DOD, DHS, we develop technologies and then we transition it out into the real world.

So years ago many of us were in avionics in another very large company and we did separation architectures for aircraft and there we are seeing with our separation architecture and our good solid programming, we were generating code 10 times faster than what the competition was able to do and that's per line of certified code. We're talking end product, the stuff that is actually flying, 10 times faster because you rely on that separation architecture.

You also end up with the ability to when you have the separation architecture perform updates, because I can update this security component and I can guarantee by inspection that it's not affecting my safety component over here, so it's very easy to do those updates and not affect the rest of the system. So it's great. What could go wrong with this and this pitch isn't actually about Isosceles, it's about gaps, what are the extra things that we need to deal with.

So you see where this architecture here, it goes down to that separation software and we're relying on commodity things. Open security issues that are out there include untrustworthy subcomponents. Okay.

We were using a separation layer, it's called SEL4 for those folks who are interested in, that's a separation kernel that has provable properties of security goodness; okay. I still have to run that on a processor. And guess what? I don't get goodness out of processors right now, certainly not the commodity side.

Now, some of your large medical device companies they actually know what's in the processor and they know all the firmware that's running at the low est level on those processors. The large companies can do that. They own everything. They buy the IP, they build it, okay, they understand and that works great. All these other small medical device companies they can't do that. They don't know what is in there. They have to acquire processors and boards and the board support packages and other things on top of that. Can I trust that? Well, I don't know. There's, you know, code up here talking about hard drives being compromised. So the actually devices that you're plugging in and putting into your systems you don't know what's running on there.

So if you look at your cell phone for instance, everybody has a cell phone. You have had little micro SD cards that plug in there. That micro SD card is just like a hard drive. It has a controller on there and it has firmware running on that. And that can be compromised and it has been compromised. Everything that you plug into these devices whether it's externally plugging in or you have it on the inside there's issues with that. You don't know what all those components are. Can you trust them completely?

So how do you build a trustable system on top of these questionable components? Things like that separation kernel they help. They help pull things apart, but it's not necessarily solving the whole problem. So DARPA a few years ago, they said, okay, we're going to do a clean slate. We're going to start from scratch, we'll build processors and other cool things up from the bottom now that solves everything in the medical device space; right? Yeah, no, not really.

One of the core issues that's still out there and Ken and several of the other speakers talked about this is the whole user authentication problem. So we're developing requirements as part of Isosceles and, by the way, with Isosceles we're giving away, we're going to open source, the requirements, the model base system engineering tools, the designs, the examples, everything, we're going to put it out there so people can just pick it up and use it. So we thought, okay, we're going to review it, so we had one of the expert reviewers here, you know, Kevin Fu, everybody knows, went into our requirements part -- one of his observations was, guys you had passwords in your requirements. Don't use passwords. Move forward, you know, get on with the new technology.

The problem is this product whatever people build on top of this Isosceles platform it has to work in the real world with real users. I'm not just going into Kevin's environment at the Mayo and just supporting them. I have to make devices that can work with patients and that includes ultimately and we're not talking Isosceles here, we're talking industry wide implantees. How do you authenticate who the user is if it's an implanted device? There's some pretty scary stuff going on with implantable devices where people are explanting them and cleaning them, they wash them a little bit and chuck them overseas and they, you know, implant them in other people. How is that implantable device supposed to know that it's now in a new person so when it gets back on the network it doesn't get reflashed with somebody else's requirements?

You also have caregivers. You have the trained caregivers, you have the untrained caregivers when people come home. How do you authenticate those people when they're dealing with the PCA pumps at home or the other infusion pumps at home or the bedside units at home?

You, of course, have all your health care professionals, but it can't design my user authentication, the health care professionals just at the Mayo. I have to be able to support those people that are in rural clinics and I also have to support the EMT personnel, there's a lot of EMT personnel in there. How do I authenticate them when they're dealing with either implants or other things that are in that home environment that they might be going into?

So that's -- user authentication is a basic problem and it's not just for medical devices. We see this with avionics, we see it in process control. We see it in everything domain, but we need basic research in here and then some standards so that the medical device companies know which direction to go.

Interfaces are a basic issue with all of these devices. So this is just a nice picture of a pretty pump in there. I'm not saying anything about this particular pump, but every interface on this device, now Kevin talked earlier, you have to assume that the environment that you're going into is insecure and that the networks you're attaching to are dirty.

In a good HDO, okay. The wired network is under the control of the HDO, maybe the wireless network is under the control of the HDO and this is just came out with a great guideline that's nice and short, 354 pages on how to secure that, just that one wireless network in there. Okay. Look at all the other networks that these devices can be attached to. And I don't know of any that are attached to all of these at the same time out there, this is just an example, again, but some of these networks are not under control of the HDO, they flat out aren't and especially when this device goes home or is in a rural clinic. The one thing that's frightening is, you know, we keep thinking of that great Mayo goodness of we want to be in that environment. We have seen medical devices on guest networks in rural network or in rural hospitals. That's terrifying. You're on the open Internet basically at that point. Somebody went in, they needed to make it work, they configured it maybe to do an update and they left it there. That's terrifying. But these devices also might come with cellular networks embedded in them. Nobody controls those things. You also have all these memory mapped IO networks that are on these things. People keep on using these new technologies. That's terrifying. Something like Thunderbolt, you can go down to the absolute lowest level of that machine and reprogram that, reflash it.

So part of the issue is people are developing new protocols without security as being that first level requirement. Dan talked about that earlier. These new protocols coming out in the future must have security up at the beginning and that goes for any type of interface that's out there.

Just heard this quote a little while ago and it's something to consider. All the medical device manufacturers here and it's not my quote, Sergay [ph] I don't know if he's here today or not or he couldn't make it, unfortunately not, his perspective is that to an attacker every single interface on your device is just like a virtual machine that that attacker wants to write things and get it running on your device. Every single interface. It's just a computer for that attacker to use and try to make it do things. So that says limit the number of interfaces you have on your machine, but then we also need basic research. We need, how do you develop interfaces that are actually secure? And that goes for any communication protocol that goes on top of these things.

Now, a reasonable question is why did these devices need so many interfaces? So I'll dive down here in a sec. The risk out in the real world might not be what you think it is. So I apologize to clinicians, EPs if they're in the audience or listening in, anybody with a better clue than I have, but the basic issue with or the basic approach to installing or implanting a pacemaker is make a cut, open a pocket, slice a blood vessel, thread a lead down into the heart, crew it into the heart, put a device in, attach that lead to it, screw it down, stuff all of that back in that little pocket that they made in the chest and then before they're done they want to test it, make sure it works and then they zip it up send the person home and then they monitor it, you know, every six months, the person comes back in, they double check on it.

So in a modern U.S. based Cath Lab, well-trained individuals what's the biggest risk that's in there of that whole procedure that outlined? There's a clue up on here. It's infection. Okay. ECRI they have a top 10 list of what are the big issues out there. Infection, it's still an issue even in the U.S. So what the medical device manufacturer said is wait a minute, remember the -- we said we had to test that device, so historically we use inductive communications, it's great. It's basically security built in, because the signal doesn't propagate very well. So I put this wand over the chest and I can communicate with that device, make sure it's operating properly and everything's great, patient goes hope. Every single device that goes into the sterile field has a potential for carrying infection, everything single device.

There's numbers associated with that. There's real risk. So they said, okay. We can make this RF, we can get rid of the device, we can actually reduce risk to the patients based on the real numbers, what we've actually seen, evidence-based medicine. They're making it better for people. Problem is the protocols, we talked about that, they're not designed inherently for security up front. People aren't coming at it that way.

The medical device companies are doing the best they can, but they need academic research. They need these protocols. They need the technologies that they can leverage so they're not inventing all this stuff from scratch. But what the medical device companies are trying to do is reduce the real risk that people really see out there, so they're adding these interfaces to make things better for folks. So academic and industry, the rest of it, the folks that feed into the medical device industry need to pick up the pace and provide those secure solutions into environment. Otherwise we have to wait and tolerate risk out there.

Now, one of the basic issues that's still out there is where does security and safety meet? And we see this with airplanes, we see it in process control. All these other industries, they have the same thing, you want to have positive control especially for situations that are abnormal. Bad things are going wrong. Ken mentioned it. This is break glass. Now, the break glass analogy isn't necessarily great, because there's somethings that you can do, you can break glass, but then you have to explant the device or do other things that are tremendously expensive and have other risks associated with them.

So how do you provide control to the authenticated person who has the authorization to do whatever that is without opening up security risks for the unauthorized people, the unauthenticated people to do things? And safety isn't intrinsic in a device. So take your infusion pump, when it fails should it fail on or should it fail off? It all depends on how that device is being used right then.

In the case of a defibrillators, what is intrinsic safety there? Should it always try to convert an arrhythmia? What if they're in a situation where they're with an EMT and somebody else is working with the patient at that point? They might want to turn off that capability in there.

Now, there's solutions for this and industry has done a great job so far, but are we doing enough? Each one of these things will provide the ability to do positive control in the abnormal situation where opening security risks and there are not solutions for that today. There flat out aren't and certainly across the board for all use cases and all domains. So we need some basic research to figure out how we can do that and get it to the right people and we have to keep in mind it's not just the clinicians in the nice hospitals, it's EMTs and other folks who need that access in an emergency situation.

There's also a concern, what are clouds doing to us right now? Now, several years ago a bunch of the large companies they did some fabulous things. So essentially with the implantable side they put units in the home. They could upload information and they could track these devices now at a much higher rate than what we could normally do with the visit and touch that patient and their device every six months. You catch all sorts of latent issues. You also can collect other data that's very useful and again, with a goal of increasing quality of life and extended life.

Now, at the time those were all private clouds. They were well-controlled. You had good solutions. You had great security around it. Then the CFOs got ahold of it and started looking at things, like, well, hey, we got AWS and other cloud providers and they're really experts at running clouds and you have presence, points of presence all over the place, so you get good connectivity. So let's go use these public clouds. The problem is how do you know that your data is where you think it is and how do you know that nobody else is looking at that data so that's a breach issue. And then how do you know that the integrity of that data is being maintained? That's the really scary one from the integrity safety perspective in there. I worry about integrity. You don't know what the -- who the support personnel touching this, you don't know the physical access to that information that's out there and you actually don't even know where that information resides. And of course there's machine to machine attacks that are going on in the cloud right now that they really don't like you to talk about in there.

Now, I've seen solutions. Well, we have service level agreements in place. We're HIPAA approved. Well, HIPAA doesn't say anything about the integrity of the data and we've also seen large cloud providers completely ignore the service level agreements and do whatever they want to do with that data. So we don't have good solutions in that public cloud space except for you can store all the encrypted data you'd like up there, that's fine. I'm okay with that. And just pull everything down and do the processing on your private cloud that you can manage, but that's not what they're selling. They're selling do all that big data processing up there and we don't have safe, secure solutions for that yet despite what the service level agreements say.

Jeremy asked about this earlier on the education side. You know, what are the issues that we're seeing and flat out basic issue, IEEE did an article on this is academia is not requiring, they are not requiring the academic institutions to have your computer science -- scientists come out with a security background. Only three organizations actually require that in there and this was done a couple years ago, so maybe it's gotten a little bit better in the meantime, but no wonder security is in the deplorable state that it is, because kids aren't coming out with that security background as their core entrenched training. They're coming out with the consumer level stuff. They know Java. They know how to do web pages and that type of thing. They don't know how to build secure products.

Now we are seeing a lot of IT professionals try to come over into the safety critical space. And it's a start, they understand some of that confidentiality perspective on there, because that tends to be their focus, but the integrity and the safety focus is missing. Once again, you don't just simply reboot these devices and hope that things are going to come back the way they're going to come back. So we do absolutely need more education in that security space and we need to push down to that lower level so that even your bachelors are starting to pick that up when they're coming out.

Then this want-to-be this is a classic case of we need used by dates. We need an agreement in the industry in terms of what they mean and how to work with them. And I was terrified to find that some medical device companies are still selling devices with operating systems that have been out of vendor support for years. And I can understand an organization, an HDL buys a device and they expect it to actually be able to function when it's in the organization. They have to figure out how to maintain that, but to still be selling it past the used by date where the vendor of the operating system says, no, don't do this anymore, I'm not quite sure why that's going on. And there's just an article in Minneapolis Star Tribune, one organization, Hennepin County Medical Center, it's a good sized hospital, one of their devices they have to update, they figured 200 grand just for that OS level. They didn't give more information, but it certainly sounds like, you know, an OS level update that they have to do.

So it's a tremendous cost for the HDOs to continuously update these things. We get that. But on the other hand, some of these devices are frankly past end of life. The architectures don't support patching anymore. They just must be upgraded in there. And there has to be some recognition for how to do that.

And then summary of the points that I hit, the untrustworthy components, end of design life and we need to do security in highly constrained environments, especially on the implantable side. So Isosceles we're focusing on bedside units. The implantable world, much more constrained. Much more difficult. Very tight living space in there, so we can't have that same expectations of that that bedside and the big devices down to the implantables. So thank you. Questions.

DAVID CODIFF: Hi, David Codiff [ph] Mills Peninsula Health Services. One example where user authentication can be difficult is in a device for a person with diabetes who might be hypoglycemic and they need to check their blood glucose level, they can't remember a password.

TODD CARPENTER: Yeah, there's a bunch of issues like that where the passwords don't work, so you want to use cards, well, what if you lose your I.D. card and you still need control?

So people often talk about well, use biometrics. Biometrics solve everything. In many situations things like thumbprints or fingerprints don't work or irises and other -- so it's not solved. There are no easy solutions out there yet. I appreciate that example. Thank you.

DINESH PATWARDHAN: Okay. We have no more questions. Let's thank our speaker one more time.

TODD CARPENTER: Thank you.

DINESH PATWARDHAN: Our next speaker is Anura Fernando. He's the distinguished member of technical staff at UL where he's been there for almost two decades. He's going to talk about hygiene, Security Hygiene for the Medical Industry.

SECURITY "HYGIENE" FOR THE MEDICAL INDUSTRY

ANURA FERNANDO: Okay. Thanks. I want to start off by thanking the organizers for giving me the best slot on the line-up, right before lunch. And I'm not kidding. When you're right before lunch, you can get the audience to interact with you and the slower you are to respond the faster you have to eat later.

So with that, I'd like to start us off with a question. How many of you are here because somebody, your organization, your boss, whomever told you cybersecurity is a big problem, you have to be there, you have to figure this out? Nobody. So we all thought there was nothing better to do on a day like today? Remember if the hands don't go up its -- lunch comes a little later. Okay.

How many of us here are engineers of computer scientists? Okay. Good, so we like to solve problems. So let's ask ourselves a question. Why are we really here today? Okay. Are we here because of cybersecurity, because people are hacking our systems? Seems like it; right?

But let's think about this problem a little bit differently. If we want to think about the whole spectrum of research solutions that may support, you know, some of the activities of NSF, DHS, et cetera that we are talking about at the beginning.

So if we really think about why are we here today, it might have to do with health care itself; okay. So we see that health care is not able to really keep up with the demand currently and so what that means is that as we get sicker and sicker as a population and there are a variety of reasons for that then the strain on health care is going to become greater and greater.

And none of us are ceasing to get old and so we continue getting old and we see some stats here that over the next couple decades a significant portion of us are going to be pretty old and unfortunately with age comes some of those chronic health issues and so for -- we are looking at the previous slide.

And, of course, you know, as we have to deal with these issues, the costs of health care keep going up and up; right. We have to deal with all these care issues and so forth. So the real reason we're here might have something to do with the state of health care.

And so as engineers, computer scientists, et cetera, we ask ourselves how do we fix this kind of problem? Well, every good engineer now knows how to use a computer; right? So we throw a computational power at this. We've got all kinds of devices that we can use to start building solutions and these devices can be found all over the place, you know, you go to any part of the world and you can find some level of computing power.

And so the technologies that support health care with some of this computational power is becoming much more widely available, much cheaper, much more reliable and much more functional and so we're seeing that technology is really potentially a good path for us to take with this less than optimal situation we have with health care.

And so as we look at innovating what these cool computing technologies and so forth we're actually able to potentially take some of the strain off of the clinicians and the people that are delivering health care by using things like telemedicine to gather patient data when people are at home, you know, and feed that into the health care process and so forth. We're able to take a little bit of the burden off of clinicians by giving them clinical decision support tools and data aggregation tools and data analytics tools of different sorts and so forth.

And so this approach of throwing technology at the problem and using computers and software has really gotten us somewhere. And so interoperability is really the key to this, because if all these different parts and pieces of technology work together, well, then we're in good shape. All these systems are going to work well; right?

And so as we have different organizations at developing different pieces of these technology ecosystems the technical interoperability is just a matter of getting the right organizations to do business together and work together and put together these ecosystems.

So problem solved; right? So, okay, we can go do too lunch, not quite yet. Okay. So let's think about why we're really here again. So when we have this kind of ecosystem, you know, we thought a lot about what are the use cases, but when we were trying to push all this out rapidly and get all these new cool technologies out and start fixing the health care problems, we didn't necessarily think hard enough about all of the misuse cases that are reasonably foreseeable. Okay. And so this is an inherent issue that comes along with rapid adoption and deployment of technology.

And so when we think about these misuse cases, you know, we've seen over the past several presentations that there are a lot of bad things that can happen and we've seen over the last several days that there are a lot of bad things that can happen. And so people are out there looking at what's exposed, what information is exposed on the networks about the product? How that information is moving through the networks, how it relates to the critical operations of the product so that if you want to do something bad with that information you can. And understanding how bad that thing can be is really relative to what the malicious user wants to accomplish. So if they want to hurt somebody, you know, there are inherent risks associated with medical devices. It's one of the few places sometimes you have to do harm to do good; right.

And so there's a financial motivation often and holding ransom, for example, that which we hold dear, our individual safety, and we'll see a little bit later it's not just about individual safety either.

And so when we create these clinical decision support systems, these big data analytics and things like that, we can see that we're creating buckets of targets for people to go after. These have value for different reasons. Some of it might be IP and people trying to compromise IP. Some of it might be financially related things like insurance. Data and things like that that can be used fraud, but we're essentially creating these pools of targets from an attack perspective.

And so we saw before that interoperability is really the solution to the technology approach;

right. But we also see that those same elements that we see in interoperability are the very same elements that if misaligned, you know, if you don't have all the organizations in that ecosystem thinking about risk the same way, thinking about how they're going to score their vulnerabilities in a common way like we heard earlier what the new adaptation of CVSS and things like that, how they're going to use tools in similar ways to analyze the products and evaluate vulnerabilities in products and so forth and now you start building the technical foundation of these ecosystems. Those are the places that these bad actors are going to go after.

And so we see that the IOT cyber threat is huge, you know, we know that. That's a large part of why we're here. Okay. And we see that it's not an inexpensive endeavor, you know, dealing with the attacks themselves.

And so we need to think about what is different in health care and what do we need to do a little bit differently in health care then maybe we have to do sort of across the board, you know there are a lot of commonalties across industries with dealing with vulnerabilities and so forth.

So patient safety is the most important asset and we've heard a lot that, you know, people aren't going to try to hack into your device necessarily to try to kill you, but if you are trying to get critical care and they were now making it impossible for you to get that care through ransomware, through what have you, now they're still impinging that same kind of threat of harm against you.

And it's also not an issue of individual patients necessarily. Now if you're looking at a clinical study, something, a product that could save hundreds of thousands of lives potentially and you compromise that clinical study, you've now effected many, many, many people.

And one of the things that makes this problem particularly difficult in health care is that we have as we know a very diverse risk profiles. A tongue depressor has a very different risk profile from a therapeutic linear accelerator; right?

And so when we look at scoring our vulnerabilities and understanding the nature of our vulnerabilities and building metrics around these processes we really have to struggle with, you know, what is the risk? What is the benefit? What is the application of my device, et cetera and it's not an easy thing.

And as we alluded earlier, another big thing is we relied heavily in the past on the practice of medicine, so I've noticed we have several physicians out in the audience and they're saying are the robots going to take over my job? Well, not quite, but we're seeing clinical decision support systems, artificial intelligence systems, things like that that are starting to shift the fundamental art in balance of the practice of medicine. And as part of that we're also seeing medicine moving from the hospital into the home and it's these computational technologies that make that possible.

So where do we start when we're trying to tackle this problem, you know, can we do some things as basic as washing our hands to prevent the spread of germs which has been analogy going on for a long, long time with our colleagues in the audience or epidemiologists and other forms of health care providers.

And so the first thing to think about is, you know, we've spent a lot of time as a community working with our leaders like NIST [ph] and so forth to think about how we're going to deal with this and we've seen and the more recent changes in this cybersecurity framework that we need business justification of this as well, because that's how our society operates. And so that's a critical piece of all of this. And when we look at the problem it's important to look at the whole socio-technical system end to end. Yes, you may have a product that fits into one place. Maybe it's a connectable device. Maybe it's interoperable with other things, but understanding what are the underlying enabling technologies where the protocols are being used for communication, what are the connectivity solutions for health care, things like HL7 and so forth. And every step of this way, it's important to think about where are there opportunities for vulnerabilities? What do I need to think about mitigating? What do I need to build into my threat model, et cetera?

And so again, when we look at this from an interoperability perspective, yes, you know, we're building this pyramid, this ecosystem of interoperable things that are going to help health care, but as we do this, as we think about, you know, moving from no interoperability to having this connected system that can help us have people go home sooner from the hospital and things like that and we start building these systems as engineers, computer scientists and other folks that are out there that contribute to this. What do I need for technical interoperability? What do I need syntactically, semantically, pragmatically, as the system changes? And these are the exact things that the hackers are out there looking at. If my system is going through a state transition, does that open up a vulnerable little window for me to get in and attack it and take over the system? And so as we build we must also defend.

And so building security into the core process itself, into the software development process is an extremely important facet of this. And we can see there are all of the points in a traditional development cycle can incorporate security.

Once we build the security in we want to be able to make some claims that yes, my product is secure. Yes, I've built in these security controls. Yes, I've tested it in certain ways and so making those claims carries with it making arguments of why you're claims should be believed and objective evidence that yes, in fact you can look at this and have confidence that I have done what I've claimed and what I've argue that I've done.

And so as the saying goes duck, here comes another standard; right. But these standards can all play different roles in the things that you do from day to day. Now we see a whole lot of them here, but they all tend to have a slightly different folks and they have slightly different things that you can leverage and that's why when you look at things like the FDA recognized consensus standards lists there are a whole bunch of standards there, because they all do something a little bit different that can contribute to regulatory science. And so we're going to take a look at an example of a standard that's published, it's about to be finished with. It's ANSI process, but it's very focused on repeatable and reproducible testing.

And so from a testing perspective, you know, that's one of these slices that many of these standards cover or that many of these other standards don't cover. And so we need to ask ourselves, well, what can I derive from these different standards? How can this help me? Fuzz testing, how many people have heard of fuzz testing here? Okay.

Zero days, do you like to sit and look through -- how many like to look through hacks and object code, you know, going into your device? Not very many of us; right? A couple, a couple masochistic people out there, but by in large we would like a way to quickly find potential zero days and this is a way to do it.

Similarly, we need to understand what are these known vulnerabilities in our system, so it's not just about zero days. We saw, you know, from the build materials discussions before and things like that, in particular, you know, you all, we don't talk about clients being tested and stuff like that, but Pat raised a really great company for me to talk about. Acme Company that Wile E. Coyote uses. So Acme Company might use a heck of a lot of open source libraries and things like that in their development, because their programmers are kind of lazy and that's why they're weaponry doesn't work so well against the Roadrunner.

So, anyway, understanding where these vulnerabilities come from is not just an issue of understanding your software and your development, it's an understanding of what are the open source things that you're adopting to quickly get through your cycles.

And looking at static source code and binary analysis and things like that also helps by really looking at all the execution pats, you know, where are the logic faults potentially going to be? What is the composition of your software where these vulnerabilities could exist and so forth and so on?

And then looking at what different controls are used, what different cryptographic techniques? Do you have sufficient entropies, a -- random number generator, you know a lot of details like that in terms of how do I actually build this product to make sure it's sufficiently robust? How do I test it and how do I generate this objective evidence that, yes, I've tried to address all these different kinds of technical issues.

And so even if you do all this stuff you're still probably going to end up having to update your software at some point, whether it's for a bug fix or a feature enhancement, it doesn't really matter. At some point you're going to do it. And so having the capability to deploy these updates, do patches, et cetera, but not just to deliver those things, but if those processes don't happen the way you'd like to be able to roll back and make the product safe again and make the product functional again if it's needed for patient care those are key attributes of this and can be tested as well.

And so finally, pen testing, so as Pat mentioned this morning, we're not talking about the ball-point pen being taken apart to get into your physical lock; right. We're talking about penetrating into your device. A lot of times you can, people do this as a black box, but there's also white box penetration testing. And as medical device manufacturers, we do risk assessment, we do a lot of documentation. We capture a lot of key pieces of information about the functionality. And so by providing that kind of information into the penetration testing process you can actually expedite things. You can say, okay, this is where I need to target, because this is high risk from a patient safety perspective, or this is where I need to target. This is where somebody could enter my device which is low risk through the network and pivot onto a high risk device like an MRI or CT scanner or something of that nature. Okay. And so there are ways to improve these processes and improve the tools and so forth.

And so in the health care space in addition to this testing we try to couple these things with processes that are already out there, you know, things like the existing risk management processes and standards. Things like the existing quality management systems, existing software development life cycles and existing regulatory processes and tools from government agencies and contractors like CVSS, et cetera.

And so the idea of all of this is really to reduce vulnerabilities that are out there. Reduce the malware that's out there and increase the awareness of security and the preparedness for security.

And so how this fits into this kind of a workshop is that we have a lot of security research going on out there fundamentally, you know, we need to set expectations in the market that we always do this minimum level of hygiene. Well, other than some mutations and things like that germs haven't changed a heck of a lot over, you know, the last 200 years and so washing our hands has been a pretty standard and static practice over that time period. Cybersecurity's a whole different story. Here we have to have an ongoing process of working with the security research community, mapping those things into industry practice tools, like CVSS, CWSS, KPAC [ph] et cetera and then migrating these things into standards which set the minimum level of requirements, those things like washing your hands that should be done and continue to evolve as we learn more and more about the threats in this space.

And so hopefully by the end of this workshop we'll come away with a better understanding of what tools need to be migrated through this process from pure research to becoming industry practice and turning into those common things that we do like washing our hands.

So thank you. Hopefully I didn't cut too far into your lunch. I'll take questions.

DINESH PATWARDHAN: We have time for one question.

JULIAN GOLDMAN: Thank you. Julian Goldman from Partners Health Care Mass General Hospital. Anura, that was a wonderful presentation. We often people don't put interoperability and cybersecurity in the same sentence, same paragraph or even the same page and I think one thing that I think about and that we've -- a number of us have experimented with is the implications of the way we connect things together to today, things that were not designed to be interoperable that the manufacturers didn't build or intend to be manufacturer -- interoperable, so they're integrated in some fashion versus things that were designed from the ground occupy to be interoperable.

So we can monitor the status of computers, for example, on our network, that's possible to do from an IS perspective and yet because medical devices are integrated today with various solutions, but they weren't designed necessarily to be interoperable from the ground up, we can't assess those devices and do those things, so I wonder if you, you know, have some thoughts about that difference between interoperable devices intended to be such versus those that are integrated?

ANURA FERNANDO: Absolutely. Thanks. Thanks for that question. So, you know, we saw the pyramid, the socio-technical system pyramid, as well as some of those blue diagrams that show the different layers of what it takes to become interoperable and so just like security if you don't bake interoperability in then you're going to have cracks between those levels that could potentially be exploited. And so while, you know, as a society, we need to go through that transition process thinking really hard about how you put compensating controls around those cracks initially as you evolve into baked in interoperability just like baked in security. Those are some of the things that compensating controls based on a solid understanding of where those cracks are, I think is important.

JULIAN GOLDMAN: Thank you.

ANURA FERNANDO: Thanks.

DINESH PATWARDHAN: Let's thank our speaker one more time. I know I'm standing between you and lunch, so I'll just take a minute or so. Over the last couple of hours we experienced some fantastic presentations.

I want to encourage you one more time to be involved in the afternoon breakout sessions, because that's where the work gets done. The discussions are captured and that's where it gets captured in the report.

We need to empty this room completely, because this will be broken up into two discussion rooms, so please take your belongings. There was a typo in the brochure and this is the, please.

UNIDENTIFIED SPEAKER: This is the actual organization and room assignment of the breakout sessions, so if you have breakout session one pick one, 1.1 or 1.2. Similar for two, three, four, five and six are on the other hand held in smaller rooms and they're somewhat smaller sessions. So this will stay up even while the room is being reconfigured, hopefully and now it's time to get some of the real work done. The real work of this workshop. I do want to take a moment to thank you the FDA as well as all the organizers behind the scenes who have made this possible, but are not are here to receive our thanks, nonetheless.

- - -

(Whereupon, the proceeding was concluded

at 12:27 p.m.)

- - -

CERTIFICATE OF NOTARY PUBLIC

I, Michael Farkas, the officer before whom the foregoing proceeding was taken, do hereby certify that the proceedings were recorded by me and thereafter reduced to typewriting under my direction; that said proceedings are a true and accurate record to the best of my knowledge, skills, and ability; that I am neither counsel for, related to, nor employed by any of the parties to the action in which this was taken; and, further, that I am not a relative or employee of any counsel or attorney employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Michael Farkas
Notary Public in and for the
State of Maryland

CERTIFICATE

I do hereby certify that the aforesaid hearing was transcribed by me from an audio recording to the best of my ability; and that I am neither of counsel nor kin to any party in said action, nor interested in the outcome thereof.

WITNESS my hand and official seal this ____ day of ____, 2017.

____

Janine Thomas

Notary Public