[00:00:10] Michael Roberts:
Welcome to the Health Connective Show. I'm your host, Michael Roberts, and I've got Justin Bantuelle, the company's COO, here with me today. Our guests today are Jose Bohorquez and Mohamad Foustok, the President and Chief Security Architect of Bold Type.

Jose's been on our show before, Mohamad's been on our show before, so guys, thank you so much. We really appreciate you coming back on to talk about this stuff today.

[00:00:32] Jose Bohorquez:
Good to join you, man.

[00:00:33] Michael Roberts:
Absolutely. So let's get into, we're going to be talking about some recent updates to the FDA's cybersecurity guidance and what that actually means for medical devices.

As we were starting to pull together some of the notes for this show, I was pretty surprised at how significant the changes appear to be. And I'm going to let you guys get into, some of the describing, how significant those changes are. But, I'm just going to throw this out there and let either one of you guys tackle the question. What is the new cybersecurity guidance? What all does it entail so far?

[00:01:03] Jose Bohorquez:
Yeah, I mean, so there's some history here. The FDA obviously cared about cybersecurity for a long time dating back to 2014 and 2016. They had some preliminary guidances around information that would be required in pre-market and post-market, pre-market submissions and then post-market once a product has been on the market.

But what happened in 2023 is that responsibility, and the statutory authority for the FDA became codified, in what's called FDORA, so the Food and Drug Omnibus Reform Act. And so there was a section added to the Food and Drug and Cosmetics Act, section called 524B that now requires the FDA to really just look more closely to what medical device companies are doing for cybersecurity, and it required medical device companies to put in place additional controls that result in enough assurance that the device is going to be secure from a cybersecurity standpoint. So, that really changed everything.

And by March of last year, the FDA released a new guidance document, around pre-market submissions and what would be required in any new submissions for FDA.

[00:02:00] And, the headline or the bottom line there is just that the bar was raised substantially. First of all, FDA began to look at, what is a cyber device or tried to provide better understanding of what is a cyber device. And it's a very broad definition. So they pretty much, they boil it down to if a device has any means of connecting to the internet, then it's a cyber device. So it's not just if it does connect intentionally to the internet, maybe it's got wifi or cellular, you would think that's a cyber device, but you might consider a medical device that just has a USB port and is not intended to connect to the internet to not be a cyber device. What FDA said is no, if there is any foreseeable means by which the internet can connect to this device, then it is a cyber device, and that means that this set of documentation and analysis and controls must be in place. When we say that the world really changed from a cybersecurity standpoint, that's really been the main driver.

[00:03:13] Mohamad Foustok:
And in fact, just to add to that March of this year. So just a few months ago. They actually already issued an update to that guidance that came out last year, further broadening the definition of the cyber device to the point that if it effectively, emits anything electromagnetic, or it has a physical wire exposed on it, a physical port somewhere on it, it's a cyber device. It's going to be very challenging to find a device that isn't a cyber device.

[00:03:39] Michael Roberts:
Absolutely. And just to recap and just to refresh everybody's memory on what Bold Type does. If you could give us like a quick plug on what it is that you guys do, and then after that, like, what does this mean for your clients now? How are you having to change how you're advising clients? How does that process look today with the newest guidance in place?

[00:03:58] Justin Bantuelle:
Sorry, if I can add something right in before that, am I correct in that a practical consequence of this is how software receives updates as a result of it? I think that's something that we're going to dive into quite a bit, but that's like a major consideration, right? Is how you're pushing software updates, because this changes the landscape of, what your obligations are as a, online device, is that correct?

[00:04:23] Jose Bohorquez:
Yeah, no, absolutely. And in fact, our interpretation, our reading of this is that FDA is effectively making it a requirement to incorporate the ability to remotely, update software. The reason we say that they don't explicitly say it in those terms, but, it's not just pre-market, what are you doing to prepare a submission to FDA? But there's now requirements post-market that you continuously reevaluate your software bill of materials to detect if there's new vulnerabilities. And if there's significant vulnerabilities that arise, you need to have a means of patching or updating the software in the field.

So, from a practical standpoint, what are your options? You either recall the devices, if you don't have a means of updating them, or you send a technician to hospitals or what, like people's homes. It just, it doesn't make sense that you're going to be able to fulfill those requirements without the capability of updating them remotely.

Now, of course, having the capability to update software remotely in and of itself creates new vulnerabilities, potentially, you have to make sure that you have secure means, and Mohamad, I'm sure can get into this in a lot of detail, but, so that's where the bar is continuously is being raised because now, you have to have a means of updating them, but oh, by the way, you have to make sure that there's a secure means of updating them. And it's not that that's unheard of or impossible. Of course, that's quite doable. But if you don't know what you're doing, you're probably going to screw it up.

[00:05:51] Justin Bantuelle:
And also if your device now falls under this category and you didn't really roll it out with that plan, now you're having to scramble, right? Like a lot of people are having to take on a lot of extra work now that they maybe didn't have as part of their product roadmap. Is that right?

[00:06:06] Mohamad Foustok:
And what we've actually found, Justin, is that, yes, for those devices that were released prior to the guide, that were cleared prior to the guidance, they've sort of gotten grandfathered in effectively.

However, as soon as they have any update required, because it doesn't have to even be a change in device.

We've had a situation where it was just the change in the intended use. FDA turns around and basically says, okay, now you have to be compliant. So that device could be out there in the field for five years or more and hadn't thought about any of this all of a sudden has to meet all the new burdens.

[00:06:41] Justin Bantuelle:
Yeah. Yeah. It seems like it's a very far reaching issue. I know I was just talking to a client today who was going through this process and just how much that's derailed where they thought they were going to go in, 2024 for their product, because now they've had to stop and get their ducks in a row on this front.

[00:06:57] Mohamad Foustok:
I don't know if Jose mentioned this specifically, but I know you asked Michael and Jose, you can give an update on what we as Bold Type do, but, before we get to that, one thing also that they added, which is another interesting sort of elevation of all of this is the FDA actually has put in place a refuse to accept policy now. This was actually put in place and became active last year, where effectively a submission is initially reviewed specifically for, cybersecurity, documentation and capabilities, et cetera.

And the FDA actually now has the ability to refuse acceptance of the submission. Prior to even reviewing it further from a medical perspective. So you can literally, have prepared your filing submitted and thinking you've met all of the requirements from a clinical perspective. And then just get stopped before you even go forwards because of lack of cybersecurity or lagging cybersecurity.

[00:07:57] Michael Roberts:
That makes it tricky.

[00:07:58] Jose Bohorquez:
To close the loop on your earlier question, Michael, so we've been around for about 7 years and from the beginning, our focus has been wireless and cloud connected medical devices. In the last year, we've narrowed that down even further to really focusing on developing secure software for medical devices and providing cybersecurity consulting to clients.

So, if it's our clients, of course, we're developing the full system. With cybersecurity in mind, putting in place the controls, all of the analyses, the documentation, everything else for cybersecurity. But even for clients who we're not doing the software development for, we just see this as such a need that we're offering that as a service as well.

Frankly, the best time to start thinking about cybersecurity for medical device is early, because if you make certain architectural decisions early, that then bring on vulnerabilities, it's going to be very difficult to meet those needs down the line. Right? So, you don't want to be in a position where you're trying to do remediation on the cybersecurity front, because it's not just a question of documentation.

It may be a question of architecture. And if you have vulnerabilities that are unacceptable, you don't find them until, a month before you're planning to submit your 510(k), you may have to go back and rearchitect your system, redevelop the software, revalidate the system, and, depending on what you're changing, could potentially impact a lot of things, including usability testing and, God forbid, even like efficacy, human studies and that sort of thing.

So, you really want to, think about that and make sure you've got eyeballs on what you're doing early. And that's one of the things that we're doing now. So secure software development for medical devices and then cybersecurity consulting as well.

[00:09:38] Mohamad Foustok:
Yeah, the phrase that FDA is now using is, “the manufacturer must provide a reasonable assurance of cybersecurity.” And that assurance is reviewed and I actually posed that to the FDA directly in a recent webinar that they had. And their statement is that they will review cybersecurity, all the documentation information you provide in the same way that they review, the clinical data and harms that the device could cause.

So they see it on par at the same level. So, as they said, this is not just about putting together some generic documentation and telling, and saying, here you go. Here's the documents you asked for. It's no, this is basically no different than any other documentation that you need to do correctly as part of your development process of a medical device.

[00:10:24] Michael Roberts:
So yeah, this just seems like a big messy problem for a lot of companies now to have to handle. If you were going to just like out of thin air, pull a number, of the amount of products that are out there, what's the percentage where this just became like an emergency kind of problem?

Like, oh, shoot, everything Justin was just saying, here's somebody that had a roadmap already for the year. And now they're having to scrap that because this is their top priority.

[00:10:48] Jose Bohorquez:
I mean, our guidance is if your system has software. It's probably a cyber device, and if it's a cyber device, then you're going to need to submit all of the documentation and analysis. Everything from your hazard analysis, specifically geared towards cybersecurity, all the way, in architecture documentation, your global views, your harm views, your patchability views, like all these documents to everything like penetration testing. You know, at the end of this and your software bill of materials.

So there's a lot of deliverables that are now going to be mandatory for you. The precise percentage. I don't know off the top of my head because there's a lot of medical devices that don't have software. So if your medical device doesn't have software, you probably don't have to worry about this. But if it does, then you probably do.

[00:11:33] Michael Roberts:
Yeah. Yeah.

[00:11:34] Justin Bantuelle:
Are you having a lot of conversations? Are you hearing people realizing how impacted they are and reaching out to you guys? Are you hearing pain, like emerging from organizations?

[00:11:46] Jose Bohorquez:
Now we are starting to hear it and I think it's going to be an avalanche because

[00:11:52] Justin Bantuelle:
They're going to start getting rejected, right? They might not know yet.

[00:11:54] Jose Bohorquez:
Exactly. I think there's a lot of companies that are trying to put their head in the sand and say, “maybe this won't impact me” or they're thinking, “well, maybe, FDA is going to be pretty lenient.” Their leniency was last year. So last year from March to October, they said, look, if you're submitting, we'll work with you to help you get things in place. But by October, they had that refuse to accept policy. And now they're like, “okay, you had your grace period.” When you're submitting your 510(k) now through the electronic system, once your system has software, there's like, 13 different entries of documents that you need to upload. And so if you can't upload them, you can't even submit your 510(k). And if you try to, just upload whatever, then you're going to get a refuse to accept. So, there's a lot of companies that need it, not as many as needed realize it just yet. So, I think, yeah, there's gonna be a big. Yeah, over the course of this year and next year, I think a lot of companies are gonna be surprised.

[00:12:51] Mohamad Foustok:
I mean, medical device development does take a while. So, as Jose said, last year was a grace period. We're still in early June. If you hadn't watched what was happening and you were in development, you could easily be caught off guard when you come to submit later on in the year, for instance.

We've had circumstances where people have submitted and be refused and have to go back. So it's happening. How many? I wouldn't know, it's hard to guess, but I would imagine that anyone that submits, at this point, without the necessary information, as Jose said, I don't know how you didn't get through the eSTAR system with a submission, if you don't have the information to begin with. But if you manage to submit and you don't have the information that you need, likelihood is there's a high chance you will just get refused. I don't see why they'd be lenient with some people.

In fact, the one criticism I may have, or not criticism, but just observation, perhaps is that FDA has leveled the playing field in the sense that although the guidance does state that ultimately the manufacturer needs to make decisions based on risks, they have raised the bar significantly whereby I don't think you can just make the claim that you are a low risk device, therefore you are exempt from all cybersecurity. It doesn't quite work that way. They're expecting you to go through the analysis and give them the information regardless.

And I suspect that the early refusals are coming because, people trying to basically say, my device is low risk, I don't need to do any of this. And I think I wouldn't be surprised if they're getting caught off guard with that.

[00:14:26] Michael Roberts:
One of the things that we talked about, around all this is like, hey, they're viewing the cybersecurity need on par with all of the other sort of prerequisites. So from the period of last year, when there

was some grace period to today, is it easier to submit the information at least? Is it as far as like the process of getting the information in front of the FDA, have they streamlined that process at all, or what's the burden level look like on that?

[00:14:52] Mohamad Foustok:
I think eSTAR, as Jose said, does break it down, pretty well. And this is clear from the guidance. And I know from the letters that people have received from FDA, FDA is very explicit as to how they want the information laid out to comply with the guidance or conform with the guidance. So I don't think there's, significant uncertainty as to what type of information is required.

Now, there's always stylistic and, level of detail questions that will come up and, those will probably be on a per case basis. But the general structure of the information, what is needed, how you need to submit it, how it all ties together, those kind of questions already are answered. The guidance actually is pretty clear.

[00:15:38] Justin Bantuelle:
They maybe aren't used to doing it. So they have to go learn something new or utilize somebody like you to aid in that front.

[00:15:45] Mohamad Foustok:
I think the uncertainty may simply be around how much should I do, what is to what level do I take this? Because obviously, like everything else, there's a cost to everything, right? So you don't want to burden yourself to the extent that now your development costs are so high you can't move forward with a project simply because of cybersecurity and it's not necessarily warranted.

So finding the right balance is important. What's enough cybersecurity that you can provide that assurance based on your risk profile that you have met or exceeded the guidance itself? You don't want to be too little because you'll get rejected and have to repeat it.

You don't want to be too much because then you're going to burden yourself with extra costs that you don't need to. I think to me, the biggest area is really this. It's as we go through this process over the next year or 2, it's really understanding where the right balance is between too little security, too much security.

[00:16:36] Jose Bohorquez:
Yeah, yeah. And FDA, just as with other areas, there is a least burdensome mentality, but least burdensome is a fairly subjective criteria, which, FDA generally sees, places the bar higher than manufacturers would. But, just to give you a little bit of an example and an excerpt because it was funny. I remember I posted a blog not too long ago on cybersecurity and somebody actually made the question like, my thing is, just like an unconnected thermometer, would that really require it? And it's funny because there's literally an example about that. And in FDA's guidance where they say, I'm going to read it to you verbatim.

They say, "for example, a cybersecurity risk assessment performed on a simple non-connected thermometer may conclude that the risks are limited and therefore such a device needs only a limited security architecture and a few security controls based on the characteristics and design of the device."

So what they're saying is, look, yeah, of course, if all you have is a non-connected thermometer, we don't expect the same level of analysis and documentation as if you've got, I don't know, like a, connected pacemaker. But they're not saying you don't need the documentation. They're just saying you need a more limited analysis, more limited controls, more limited.

So that's where I think people are going to be surprised that they're thinking, well, my device, it's not connected. It's very low risk. I don't need anything. And FDA is saying, no, you need to provide the analysis, the controls. They're just not going to be as exhaustive as a high risk device that's intentionally connected to the internet.

[00:18:06] Mohamad Foustok:
And in reality, everything does flow from that analysis. When you begin by looking at the architecture of your system and you flow down and create your threat models, identify your threats and assess them. When you go through that process and you've determined that, from there on, everything does become risk-based.

If you've identified that there are very few threats that can affect you and they score low and they are acceptable risks. You can shortcut a lot of the work you do from there on in, but you can't skip that step, right? You can't just simply ignore the analysis and just say, I have decided that I don't need this.

I think that's the point is that FDA are going to look at this from the top down and say, okay, what does your architecture show? What does your threat modeling show? What does your analysis reveal? And then what controls are you going to put in place and why because of that analysis? And I think it's all logical and reasonable.

But I think again, the mistake is probably skipping that analysis, deciding I have a low risk device, therefore I don't need any of this. That isn't going to fly. And from what we've observed, and I don't know to what extent this is true, actually, FDA does have a team that is their cybersecurity team of experts, and they are involved.

We have had members of the team in calls with us to give their input. So again, this is no different than if you were putting a medical device in and, from a functional perspective, they needed a cardiologist or they needed someone else who has medical expertise.

There are people there that will provide that. So security is no different. There are experts, even FDA that can provide, their opinion as to whether the security you're providing, is adequate or not. And they utilize that.

[00:19:57] Michael Roberts:
So let me throw a scenario at you and see if this is one that you've encountered yet, or this is something that people are trying to figure out how to handle. So one of the things that you mentioned is, hey, a company has several devices out in the field. And we'll just limit it to hospitals for now.

So they're out in the field, they're in the hospital, they're going to make some sort of change. Now they need to make some sort of update to where there is new cybersecurity protocols put in place.

Is it at all feasible to have people go out to every one of those facilities? What are their options at that point?

[00:20:30] Justin Bantuelle:
Your field service group deploying the changes by basically visiting the location.

[00:20:35] Mohamad Foustok:
It's a broad question, but let me start by saying that generally speaking, I would suspect that systems that are in hospitals already are connected into hospital networks, should already have, a certain degree of cybersecurity already. They're not necessarily because of the 2023 guidance from FDA, but because hospitals themselves have been imposing stricter security requirements, even prior to this. So I would be shocked if there was a device that was so bad that they would have such a major remediation and they're connected in the hospital system. I'm not saying that may not be, but that would be a little bit shocking to me.

[00:21:18] Justin Bantuelle:
Some of it, too, though, is that, sorry to interrupt. Now, part of this shift is that maybe the device is never intended to connect to the hospital network. But just because it was viable now, it's falling under the standard. Right?

[00:21:33] Mohamad Foustok:
That, that would be one case, right? And then it comes down to, ultimately, your question Michael, about feasibility. If this is a high-value product and expensive piece of equipment that's sitting in a hospital and there's a limited number of them across hospitals, and you're talking about hundreds or possibly thousands, not tens of thousands, then the reality may be, yes, you would have to, perhaps the only update method of these things is to physically insert a USB stick into a port on the machine because it was not intended to detect it. And so the reality is you would have to send somebody around to each of the machines to do it. As Jose said.

[00:22:10] Justin Bantuelle:
The FDA would consider that acceptable potentially though? That's where I was curious.

[00:22:14] Jose Bohorquez:
Well, it depends. I mean, what the guidance document says is that there's a rating of these vulnerabilities and Mohamad can probably get into this, what that process looks like to rate these vulnerabilities. And so there are some vulnerabilities that are unacceptable, and then there are some that are critical.

And what FDA is saying is that if a manufacturer finds an unacceptable vulnerability, then they need to resolve it within a reasonable amount of time within its regular cycle of updates. But if they find a vulnerability, that's actually critical, they have to resolve it as soon as possible.

And their definition of that is less than 30 days. And they have to actually also keep track of the percentage of the units that are fielded and what percentage of them have been updated. So those are metrics that FDA is looking at as well.

[00:23:00] Mohamad Foustok:
And metrics, and how long it takes to update, et cetera.

[00:23:03] Jose Bohorquez:
Exactly. So there might be scenarios where you've got something that's a high risk product and it's a critical vulnerability where it's not acceptable to have techs go out there with USB sticks if that's going to take six months to rule out a change.

[00:23:17] Mohamad Foustok:
Yeah, to Jose's point exactly, there actually is as part of what you submit as part of the requirements for the guidance is a plan on how you propose to do this. And so when you again, go through the process of, performing the steps necessary to conform with what the guidance states.

You will go through the exercise of determining that scenario of if a vulnerability is discovered and I need to do an update, what's my plan to go and update it? And you need to articulate that. And if it turns out, and you need to do it for yourself anyway. And if it turns out that the cost of executing such a plan and the time it takes is unreasonable. You may need to come up with a scheme whereby, for instance, you go and equip your machines with a remote update capability. You, add wireless modems to them or something like that so that you can centrally manage them. That opens up a whole other avenue that you were not expecting, so you were expecting a software update and all of a sudden you're now required to do hardware updates too. But again, perhaps if it's high value equipment, that's warranted, to be able to maintain them.

[00:24:19] Justin Bantuelle:
Right. You do it once and then you're equipped moving forward.

[00:24:21] Mohamad Foustok:
Yeah, or are you both through the process of deciding maybe I should connect into the hospital network, but then that opens you up to a set of other things. Again, it's like opening up a can of worms here. So yes, you're legitimately trying to comply, but, those steps of compliance might open up all kinds of avenues that you haven't even considered. And you have to go through the exercise of the kindle that makes sense.

[00:24:42] Justin Bantuelle:
That makes a lot of sense. Something kind of related to this that I'm curious about. Has anything changed regarding this? And we're talking about like, okay, with these critical updates, you need to roll them out rapidly. What is the process? I know that these things are highly regulated, right?

So you can't just push software updates willy-nilly, already. What kind of submissions, what kind of standard to get something out as quickly as possible to meet your obligation to update your software. But then also what's the like vetting process, a submission process. Do you say this was so important we had to release and then you backfill at that point?

What does the FDA look for from you, on this with a higher burden of get things updated as soon as vulnerabilities are found?

[00:25:23] Jose Bohorquez:
I think you're hitting on something that's really important, which is, typically people consider that if you're making a change to a medical device, you have to go back to FDA. That's not always true. It depends on the change that you're making. If you're not changing the efficacy of the product, the risk profile of the product, those kinds of things, oftentimes, you can just do a letter to file, for example. But when it comes to making changes that are related to cybersecurity threats, the FDA

recognizes that time is of the essence. And so they expect you, in fact, to have a plan in place and it's part of what you're submitting to say, if we find a vulnerability, here's the process that we're going to follow to patch that security risk. And it's not a process where, you're going to put together a plan and you're going to submit it to FDA. You're going to do all your development, all kind of stuff. And it's going to take 6 months. That's not acceptable. They recognize that. And the expectation is actually that you have a plan in place for rapidly making the modification to the software, you're developing the patch and releasing it and documenting all of that and report it. So you're not asking for permission. You're reporting post facto on the changes.

[00:26:29] Justin Bantuelle:
On what's already been approved as a procedure that,

[00:26:33] Jose Bohorquez:
Yeah, exactly.

[00:26:34] Justin Bantuelle:
But then that feeds into all of the legwork that people are now going to have to do. This is just one more thing they have to define as part of the submission process.

[00:26:41] Mohamad Foustok:
I think Justin, to maybe you answer your question slightly differently, but to add to what Jose's saying, I think when you look at functionality, and I think that this is an area that people misunderstand when you look at functionality within medical devices, in the past, there was, the tendency to basically consider medical devices as homogeneous. It's a medical device, the entire thing is a medical device. FDA shifted that language years ago, back in 2018, I believe, but the language started to shift more from medical devices to medical device functions. And there's actually separate guidance on software, medical device functions. And if you start thinking of them in those terms, if you start thinking of medical devices, not as this homogeneous lump of something that is all one thing, but in fact, if this can be segregated, and if you start creating architectures, where medical device functions are segregated from non-medical device functions.

Then you suddenly find yourself in a different situation when it comes to security because if you can treat security mechanisms as a non-medical device functions, which they often are, they could be communications related or related to things other than the medical device pure functionality. Then all of a sudden you now are in a position where you can have a different type of release cycle when you are releasing updates to non-medical device functions versus medical device functions.

So, to what Jose said, this can all be in your plan. So, your plan may be that when, for instance, I am making changes to the medical device functions, I may go through and do a clinical trial. There's a whole variety of things you may do because you're altering the behavior of the medical device.

But in that same plan, you can have it such that if I make updates to non-medical device functions, I don't need to go do all that as long as I can do perhaps a regression test to confirm that I'm not altering the medical device behavior. There's a whole slew of other things I can change that don't impact the medical device. And I can shortcut the process and be able to release them more quickly. So, this is really all about how you develop your system.

[00:28:44] Justin Bantuelle:
Yeah, that's fascinating. It makes a lot of sense. I'm mapping that to like some of the customers I've

worked with and where I don't think they have that partition. The software update to the device is the software update to the device. And that makes a lot of sense when you talk about architecting at the beginning of this call, we were talking right about how you say architecting one way makes this not that painful. Architect in another way, you're going to have a really bad time.

[00:29:08] Mohamad Foustok:
A few years ago, we started to emphasize this and started to increase the granularity of the systems so that you have very clear-cut areas of a system that are medical device functions. You have the medical device function that they call them. Then there's MDDS, which are basically medical device data systems, which are a level below medical device functions.

So they're handling medical device data, but they're not altering it. They're storing it, transporting it. And then there's non-medical device entirely. So you can actually segregate your system into these multiple domains. And now you can manage that system as these granular pieces, and it alters how you view things,

[00:29:46] Justin Bantuelle:
The value of the scene is immediately clear. Yeah. It makes a tremendous amount of sense.

[00:29:51] Mohamad Foustok:
But it does require discipline. You do need to have that discipline up front to think this through and understand the consequences. And in fact, it's desirable also from another perspective, from a pure security perspective. I've always believed that, one of the essences of good security is reducing the footprints of what you're securing. This goes back to the medieval days, like the huge castle is very difficult to protect compared to the small castle. If you have a large monolithic system, trying to secure it becomes very challenging, but if you can break it down and secure parts of it, or parts that are important of it, at the end of the day, ultimately you're trying to secure your medical device functions. That's really what we're trying to secure. You may find that anything that's outside of that is not relevant anyway to what you're trying to secure. It doesn't have any effect. Basically, if you can partition your system and you can break it down into medical device functions, you actually will end up with a much smaller footprint. You'll see that when you do the threat modeling. You'll see that you've got a much smaller footprint that you're trying to protect, which reduces the number of threats, which reduces the number of mitigations you need. Again, so all of this follows correctly if you are creating an architecture from the beginning, that is appropriate.

[00:31:06] Justin Bantuelle:
Right.

[00:31:06] Mohamad Foustok:
It doesn't help you unfortunately, if you're a legacy system and you haven't considered these things, and that's unfortunate. But if you are starting development today or are still early on in development, you really should be applying good principles of architecture to begin with, especially in this space, knowing what's ahead for you.

Knowing that, software updates are required routinely. Knowing that medical device functions are much more scrutinized than non-medical device functions. It behooves you to create a good architecture from the beginning and lay the groundwork to ease your path over the next decade, as your product is out in the market, as opposed to not thinking about it, putting a device out there and then dealing with the consequences of it.

[00:31:49] Justin Bantuelle:
Right. Or you're probably not even going to get your device out there potentially. You're not going find out until submission time, which is a terrible time to learn about that.

[00:31:57] Mohamad Foustok:
I got my tie in between architecture and security, where the two are go hand in hand, really.

[00:32:02] Jose Bohorquez:
Well, to tie it in even further. I mean, to the original question that's actually one of the architectural views that FDA is requiring is, your patchability view, your updateability view, right? So how is your system architected to allow for patchability? And as Mohamad's explaining, if you have to be able to patch the entirety of the system, that's different than if you really limit the footprint of what's critical, and you only need to have the capability of patching that.

[00:32:29] Justin Bantuelle:
Right. If a critical update could potentially influence the patient outcomes, then that's probably not going to fly.

[00:32:35] Jose Bohorquez:
Yeah, and in a way, I think some people are looking at this and generally, from a regulatory standpoint, sometimes people tend to think of okay, this is the extra work that I have to do because FDA forces me to and FDA, the, I think they're well-meaning in the end.

I really believe that. And it's the same thing with cybersecurity, it's like general design controls for product development, where you're supposed to have plans in place and user needs and design inputs, design outputs, design verification, design validation, somebody who just wants to hack a system together, looks at that and is annoyed that they have to go through all this extra effort. But somebody who's been developing products for a long time and knows all the things that could go wrong recognizes that spending time early in documenting your design inputs, what are the requirements of the system that I'm going to then verify against has a lot of value.

It's the same thing with cybersecurity. Now they're saying like, okay, you need to put these architecture views in place. If you do it as a post facto exercise, you know that you're throwing together to try to get a submission in place, you're losing out on the value that it has if you do it early in the process, because it forces you to think about the system and how to architect it to make it secure.

So if you follow the process from the beginning, you're going to gain benefits and you're going to ultimately have a system that's more secure with less work. If you try to put it all at the end, it's going to be more work.

[00:33:54] Justin Bantuelle:
Yeah, it'll be able to operate in the field for a lot longer. You're not going to be scrambling as much. You're not investing as much in the maintenance aspect of it. That makes just such a tremendous amount of sense. And then it's interesting too. The FDA is not trying to make people's lives difficult.

They're trying to make sure that people are safe. And I think we all agree with that as a critical element of it. But yeah, it's easy to lose sight or feel like this is an adversarial relationship. This

comes up a lot, too, when we're talking about like HIPAA standards, when we're doing data transfer stuff or trying to present information and the idea that like, okay, we're going to give up on that side of things, the equivalent there would be okay, I'm just going to remove all ports from my device and I'm going to try to lock it down so incredibly that I can never possibly fall into the standard.

You're spiting yourself, right? You're creating a lot of long-term hardships if you're fighting this, and everything you're saying makes sense to me. It really resonates with me in terms of, yeah, good design. It's so easy to get tunnel vision on if you're building a device, I've got a problem to solve.

I'm just gonna build to solve that problem. Well, it's like you solve your immediate term problem, but you've neglected to think about all your long-term problems you're creating for yourself.

[00:35:02] Jose Bohorquez:
Yeah. And not the least of which is what happens if your system gets hacked down the line? I mean, the potential safety implications to patients, but even the business implications. If your system happened to be recalled or all of your devices going offline because of vulnerabilities exploited, what does that do to your business?

What does that do to your company's reputation? And that's like, God forbid, if patients actually get hurt, which can happen. I mean, ransomware is definitely real. There are big hospitals, but there's also small medical device companies that are being attacked with denial of service types of attacks and all of a sudden they're sitting there literally having to send millions of dollars in Bitcoin to somebody. People think this doesn't happen. It happens. It's several hundreds of billions of dollars, approaching a trillion dollar industry.

[00:35:49] Mohamad Foustok:
Yeah, I think I forget the number. But cybercrime is a trillion dollar a year business and it's growing. There are stats out there that they're sharing together now on cybercrime. And although cybercrime in medical specifically in the US is still in the billions. It's a rapidly growing space. In fact, I think the numbers I saw was that by 2030, it's expected that within the US alone, the US will hit around a trillion dollars of cybercrime on current trajectory. And that will mean all cybercrime goes up anyway, as part of that.

So medical is only, in other words, it's only going up from here. Unless something, and sadly, like oftentimes, much of this is always too late, right? We're not putting this in place to prevent, cybercrime because it hasn't happened. We're putting this in place because cybercrime is real.

It is happening. So as Jose said, it's happening all around us and we're now trying to catch up. And so I think right now, the hope is that we can bend the curve of it. And, if companies take it seriously and really lean into this and make good efforts, it'll lessen the acceleration of cybercrimes.

It's not going to eliminate it. But it will make it harder. And the chances are going to be less that you're the party that's ransom, not that you're going to necessarily eliminate all possibility or what you can, it's the old adage of, you don't need to run faster than the bear, you just need to run faster than the guy behind you.

So we're in this position right now, companies that lean into it and take advantage of the opportunity and actually add security are putting themselves in a better position to not be the target of cybercrime. Someone is going to be the target. It just doesn't, you just don't want it to be you.

[00:37:48] Michael Roberts:
Absolutely. So guys, this is obviously a big complicated and difficult to solve kind of problem. Thank you guys for coming on and talking through it. I think like some of the big takeaways I got was, hey, even if you think your device isn't something that needs some kind of plan in place, you probably do. And then, from the start plan this stuff in and as your software and as your, security go together.

So guys, thanks so much. We really appreciate it. So Mohamad and Jose from BoldType and, for any other episodes, you can go to HC.show and learn more about us. Thank you so much.