Webinar

Navigating the New HPH Cybersecurity Performance Goals

Saul Marquez: Hello everyone! Welcome to today's webinar. We'll go ahead and let everybody get settled in for us to get started. Thanks for being here. All right, welcome everybody! Good afternoon, good morning, and thank you all for joining us for today's webinar, navigating the New HPH Cybersecurity Performance Goals. Today we have the privilege of having two hosts. And first, I want to introduce you to Ed Gaudet. He's the CEO and founder of Censinet. With him, we also have Erik Decker, Vice President and Chief Information Security Officer at Intermountain Health, also serving as a chairman of the Health Sector Coordinating Council Cyber Working Group. We're so excited that you guys have joined us today for this very special webinar. Just a reminder, everybody has access to the Q&A feature where you could type your questions. We'll be answering those questions at the back part of today's webinar. And finally, all the slides in today's deck will be shared with you, so no sweat there. The team at Censinet will be following up with those should you wish to have the slides. Thank you all for joining us, and now I'll turn the floor over to Ed and Erik.

Ed Gaudet: All right. Thanks, Saul. Welcome, everyone. As my wife reminded me, I need to update my photo here. So, probably the next webinar will be an older-looking, more distinguished Ed Gaudet. But welcome, Erik Decker, to the webinar today. We've got a lot to cover. So, how are you doing today?

Erik Decker: Good, glad to be with a distinguished gentleman like you

Ed Gaudet: Yes, thank you. Alright, so let's get started. And before we do, I have a special surprise just to keep it interesting and light, Erik, right? You don't mind, I hope, but I wanted to congratulate you for your article in the Harvard Business Review. That's huge, yeah. You didn't see that coming, did you?

Erik Decker: No, thanks for that. Yeah, this was a, so first of all, like, yeah, a little bit of a shock to be asked to write an article, which is amazing, but John Glacier and Janet Guptill with the Scottsdale Institute were instrumental in that as well, but yeah, this whole article was. Effectively, we've been talking about systemic risk and ecosystem risk for a while. And so, you know, the whole change healthcare situation that is obviously on everybody's, you know, top of mind. as with any major, you know, incident, you get some momentum and you get some opportunity. And so, we're, was asked to provide some thinking into this particular problem. I personally think that we have a significant change that we need to make with the way we do our risk analysis and risk work, risk management work. We got to get out of this myopic where the center of the universe kind of mindset and into where all nodes connected, we're all interconnected, intertwined, and we induce risk as much as we consume risk, so that's what the article is about. It has some positing in there. It has some things about minimum controls and stuff like in there. So, stuff that's relevant to this conversation, but hopefully, yeah, give it a read and hope let me know what you think.

Ed Gaudet: Yeah, and it just went live today. So, it's relevant to the conversation, obviously. And, of course, you know, I couldn't agree with you more on this incident side, so let's get right into it. So we got a lot to cover today. Let's talk about how we got here and really the why behind the work and the focus in on CPGs over the last year or so. So let's just talk about what's been happening from your lens as a CISO at a large institution, at a large health system.

Erik Decker: Yeah. So again, these are not new things. What they are accelerated and the velocity associated to the issue, the disruptive attacks that have been happening has been ever increasing. I mean, these stats here are just like even looking at the ransomware attacks, one on the right, you know, double the amount just in healthcare alone is not great by any stretch of the imagination. The records themselves is, you know, always been problematic, but you know, we all know that it's not a matter of, we know that these attacks cause major disruptive issues. We know that there are implications of harm associated to it. There's actually an interesting article that came out that studied some of the damages associated with ransomware attacks.

Erik Decker (cont'd): And, you know, they estimated patient death associated to the ransom attack through an academic study. You know, so this is not just conjecture. It's science and academics and, you know, through an appropriate peer-reviewed journal. We've also seen studies that show secondary impacts of ransomware attacks against surrounding hospital systems and regions and how very measurable disruptions have occurred, like ER wait times going up and stroke response going up. And, you know, these are all, it's not a large long conclusion to that causes harm. So the problem is, of course, you know, what do we do about this? You know, this is a constant battle associated to, sorry, it's a constant battle that we have associated to these bad actors that are out there, and there are common methods and common ways that that is occurring. We're going to see that as we get deeper into the slideshow here, yeah.

Ed Gaudet: I would add, if you haven't seen this slide, you're probably not in healthcare, right? So let's see. The other thing to consider is, this has been a growing problem over the last, you know, 3 to 5 years, you know, Censinet and the group did the first qualitative study in this area, based on some of the anecdotes we were hearing about ambulance diversions, and care wait times, and other issues associated with ransomware and, and, you know, since 2001, it's just progressively getting worse and worse and worse. And so this is, you know, obviously, something that everyone in healthcare is maniacally focused on at this point, yeah. So and I remember, you know, we talked about this a few years ago. You kept coming back to, you know, there's there's really three ways one gets hacked. Let's cover the three ways at a minimum.

Erik Decker: And this is, again, it's not based on Erik's opinion. This is based on, it was originally sourced when we did the the landscape analysis, the Hospital Resiliency Cybersecurity Resiliency Landscape Analysis that was released last April. And it was a joint effort from the Cyber Working Group and Health and Human Services. And we studied the resilience measures, so there was a CHIME's most wired survey and the AHA, Censinet, KLAS survey that looked at, I think we had about 300 systems that had participated in that in totality. And we looked at that as a measure of resilience, like there's very deep questions in there, like how like where's your multifactor? What are you doing it on? Is it on email? Is it on VPN? Is it like all these very, you know, deep things? And we compared that to the threat intelligence about how we're getting beat. And you know, the threat intelligence came from a bunch of different sources. Health Human Services, HC3 had some sources, some commercial sources like CrowdStrike and Verizon data breach report. Some, we did 25 different interviews with systems and some of those that had been hacked by, been compromised, you know, by bad actors. And the theme was consistent across the board.

Erik Decker (cont'd): You know, we we say, you know, highly sophisticated, highly sophisticated threat actors are causing these problems. What I'm going to tell you on that is that the highly, high sophistication is coming from the ability that they have to scale their attacks at the scale that they're doing it, you know, from the exchanges that are in place, you have access brokers that their entire job is, they go in, they break in, they get credentials, and they sell those credentials to other bad people on a black market, you know, and there's real money changing hands to ransomware as a service, you know, where you've got companies that are out there, ransomware companies that are just building purposely built malware that can be used or, and/or, you know, provide the services by somebody who wants to cause, you know, damage. And they get a slice of the pie, you know, from the, from any extortion that takes place to the infrastructure that they use to actually conduct these attacks and how they spin it up and spin it down. That's sophistic

Ed Gaudet: Go ahead, go ahead.

Erik Decker: Yeah, the middle one is third party, so, and it's third party, not from the, they have our data. A problem, for sure, don't get me wrong. We're not absolving ourselves of the privacy and confidentiality challenges, but it's the connectivity that we have with the third parties. You know? What kind of connectivity is it? Is it a secure API? Is it there is no connectivity at all? Okay, well, that's a less risky proposition. Is it a VPN with full access inside your environment? Whoa. That's a potentially very risky proposition. Because if they get hit, then they're going to ride those channels over to you. And once they're in, inevitably, the attack is a lateral movement. Quick, find to the IT administrator that manages your major systems of record like Active Directory, highly, highly leveraged platform. They get domain equivalent rights. And once they have that, they do their data theft. They do all, they do all, they stage everything, they leave it, and then they push the ransomware because they have control over all the assets in your environment once you get to that privileged global administrative access, and that's the attack. Every, I'm batting a thousand on this, every CISO I've spoken to that's been, that has been subjected to an attack like this. I say, don't tell me how it happened. I'm going to pull out my crystal ball, and I want you to tell me if this is right, and one of three ways and one thing that they did before it went, and it is.

Ed Gaudet: And the sophistication of this, you know, is also just to echo the point, it's their patience and the surgical nature at which they these attacks are premeditated. And they come in, and they wait, and then they or not.

Erik Decker: So it's Change Healthcare, they, nine days of dwell time.

Ed Gaudet: Yeah, but they were, they broke.

Erik Decker: They were in for nine days, and then, they did what they did, and they were out. So it's, I mean, it's yes, it used to be big patients. You know, it also depends on your adversary, right? So who is what's the goal? You have to have an adversarial mindset has to be the core of what we do. You know, who is coming after us, and why are they coming after us, and what do they want to do? You know, so if you have a criminal organization, they're going to want to, they're going to want to make as much money as they possibly can as fast as they possibly can. So they're going to hit you, and they're going to, they're going to go in, they're going to go hard. They're going to go. They're going to get what they need to get, and then they're going to extort you. If you have an actual nation state actor like China, that's a different story entirely. That is a low dwell. They're in for a long time. Deep potentially. And why are they there? You know, intellectual property theft, maybe it's a national public safety issue. There's all kinds of different reasons as to why they might be wanting to do what they do. And the methods that they use are going to be different from this. Like this is the attack that shuts down organizations that attack the nation-state attack is a different attack entirely.

Ed Gaudet: Have you seen any attacks where the insider is the vector of attack, where the insider is enabled through some mechanism? Is the launchpad for that?

Erik Decker: You mean, like they are leveraged by an outside influence or something?

Ed Gaudet: Yeah, an insider gets compromised and they, you know, there's been talk about it, but I, I've just never seen it or heard of it.

Erik Decker: I, in my career, I have heard of that happening mostly from a confidentiality and data theft perspective, you know, so give us, you know, give us a copy of every slick sheet that come or every face sheet that comes in, you know, kind of deal, and we'll come up and pay you for that, but later on. But like, again, that was like 20 years ago. So that, that's, they don't need to do it that way anymore. They've got scale at their breadth.

Erik Decker (cont'd): The other thing is, you know, don't get me wrong, insider again, what are the what are the types of attacks that are happening? What we're talking about here are extortion and disruption attacks. If you want to commit fraud, you're not doing it this way, you know, or maybe you're doing part of it this way, but like, you literally want to steal money out of your, out of the coffers, you know, you're going to go after the financial organization. You will do social engineering attacks, you know, business email compromises, those kinds of things. Those are still very prevalent. You know, you could potentially have an insider there who, you know, might have more access than is necessary and can commit fraud because of that. That for sure happens. Different type of, again, different kind of context of what we're talking about, though.

Ed Gaudet: Yeah, different vector. All right, let's go. Let's move on here. So, let's talk about the how we got here, the what, and as the poets like to say, what a long, strange trip it's been on this journey. So, obviously, you've been at the center of this from the beginning. So, you know, share with listeners, basically how we got to where we are today.

Erik Decker: Yeah. So, it all started with HICP and the 405 task group back in 2017, and there was a law called the Cybersecurity Act of 2015 that required HHS to facilitate and organize an industry-led group to establish best practices and methodologies. That group came together in 2017, in DC. It was the, it's the 405(d) task group that you might people may or may not have heard of that. And the publication that we produced was a document called HICP, and HICP, the Health Industry Cybersecurity Practices is, it posited, you know, strangely enough, the same theme carries forward from 2018 to today, which was, in 2017, '18, we were saying, what are the five most prevalent threats on how we get beat, and what should we do about it? What are the ten things that we can do about it? And let's build that based on let's build a playbook for if you're small, medium or large and give you a different path based on that, because your resourcing is different, based on who you are, what kinds of, you know, if you're a small medical practice, you're going to tackle those challenges very differently than a large integrated delivery network like Intermountain. So HICP was built and born, released at the end of 2018. And, fast forward a couple of years to public law 116 321, which was an amendment to HITECH. And what that law said is, if organizations have established what is a defined term called recognized cybersecurity, or recognized security practices, then OCR, the enforcers, need to consider that when they're doing their enforcement work.

Erik Decker (cont'd): So it's not a safe harbor that was being used at one point Safe Harbor is, you know, in place. It's not safe harbor, but what if you can demonstrate you've adopted it over the last 12 months, then when an enforcement action comes in, you are primed towards, you know, to, towards defending the case, you know, of, you know, should were you negligent or not kind of thing. And, you know, of course, we have HIPAA and the HIPAA security rule that's been in place since 2005. I'm remembering my time in the, you know, and so, and we all have to abide and adhere to HIPAA. And that is the, that's the basis of how OCR does its work. But now, you can add in anything derived from 405(d) that's in the law. So HICP is directly called out in the law as an incentive. Also, anything that's connected to the NIST publications. So you have adopted CSF or 853 or whatever that framework is, and you can demonstrate adoption to that. Those are all things that will help you in enforcement. The intention there washow we're getting beat and what what are we doing? Like, where are we at benchmarking wise? That, plus a bunch of other input from the industry and others, turned into the Health and Human Services strategic concept paper. And that was where they stated effectively, there's four things that need to happen, and in the upcoming year, one is voluntary adoption of better cyber controls, incentivizing the industry into adopting said controls, establishing minimum standards. That's the third thing. And the fourth thing was setting up a front door to HHS for all things cyber. And so that was released in December and then turn around in January, February, I think it was January, was the first version of the CPGs. And the CPGs are the health and public health cybersecurity performance goals. This was broken up into a central and enhanced, there's ten of each, and again, the same concept. This is why I find it that the model hasn't changed adversarial mindset. How are the threats happening? What's occurring out there? What do we need to do to protect ourselves? So the CPGs and HICP, they're actually completely intertwined with one another. When we were building the CPGs, it was we did not want to get rid of HICP because that is a, it's been well established. I think we have somewhere of like 3 million views on the websites. It's just a massive amount of download and industry acceptance. We have a law behind it as well, but there's some really good statements on the CISA CPGs, when you look, when you read them, like when you read just the High Line, there's like an outcome statement, you know, effectively says if you do these things like two-factor authentication, put two-factor authentication on your systems, okay. That's an outcome statement. It doesn't tell you how to do it, but it defines like a scope. And so we liked that. And so we said, well, let's just take the let's take the outcome statement and the CPG, and then we'll tweak it for healthcare because there's some nuance there, and then let's attach it to HICP.

Erik Decker (cont'd): And then right below it is HICP and the sub mappings and all that. So that, the way we also did this was it was, you know, ten essentials and really trying to fit that puzzle piece of resilience. You know, what did HIPAA not give us already, or what did some other regulatory regime not give us? And how do we, you know, if we implemented these things, would the collective resilience across the industry actually go up? That's the hypothesis, the goal, and the desired state. So the essentials are the floor and the enhanced are just another step in maturity. They are not intended to be the end-all, be-all. It is not intended to say like you do all of this, and you're done because that will not be the case. We will, we are always in this cat and mouse, cat and mouse game. We're always the adversaries are always going to shift. They're always going to. They're always going to commit crime. We're not getting rid of that, right? So as we plug the hole, there will be a new hole. So we have to be reactive to those things, but we also need to stop messing around with what we think the basis needs to be, so yeah.

Ed Gaudet: Yeah. Let's, and, you know, each one of these is designed, again, as you said, to provide that base level of protection and coverage that can not only be used in a way to demonstrate adherence, and also maybe capture some of the incentives that are available, which we'll talk about in a second, but also provide a roadmap that makes sense, right? Like start with the essentials don't necessarily go right to the enhanced, right? And then, from there, you build your program. So, any comments about that and how people should think about sequencing?

Erik Decker: So I just, you know, I want you to look at, read the words on this because we argued about the words a lot. So know that. And I know that there are I know there are doubters that say, you know, like why this and not that, you know, so nothing is perfect as first of all what I'll state, and everything was intended to if we did these essentials, do we stop the three ways in and the one way once they're in or do we take it not necessarily fully stop it, but are we taking a significant bite out of the damage of those vectors? That was the intention of these, of these CPGs. And so you'll see things like mitigate known vulnerabilities. Notice that this does not say mitigate all vulnerabilities. It says mitigate vulnerabilities, blah, blah, blah, blah, blah, directly accessible from the internet, right? It's a very clean and specific scope because that's the way in. You know, if you have a Kev on the internet and it's not patched in 24 to 48 hours, they're going to get in.

Ed Gaudet: I also ... over ten myself, identify ... and mitigate risks associated with third-party products and services, yeah.

Erik Decker: Well, that's, it's the.

Ed Gaudet: Very clean, well-written.

Erik Decker: Yes. You know, the multifactor authentication. We're not saying multifactor authentication on every single thing that exists. We're saying if it's exposed to the internet, it better be multifactor. And that means onto your network or even in the cloud, you know, if it's in the cloud, directly accessible, it should be multi-factored. So anyways, that's the that's kind of the basis there.

Ed Gaudet: Take a look at the enhanced same thing.

Erik Decker: Yeah. Enhanced is taking it up the next step. And you know, again, this is where one of those debates like why is asset inventory not in essentials. It's one of the, you know, CISA's top ten and all of that. And to that, we say yes, of course. You know like knowing knowing where your assets are and knowing how to protect your assets is very important. We've also been in this state of inadequate asset management as an industry for our entire life, you know, of everything. And when you look at, you got to go down to the lowest common denominator because the CPGs are going down to everybody eventually, the way it will work itself out through rulemaking is anybody who's in healthcare that's doing this is going to have to adhere to this. So we have to do the things that are going to be the biggest impact first, and then we supplement that with the things that will make it all better. So that's the argument on asset inventory. We had a couple of other arguments in here. I won't go into it, but like I think a few of these things could swap. It doesn't matter at the end of the day. Like if we do these 20, we're going to be in a much, much, much better place than where we are.

Ed Gaudet: Well, I think your point about HICP to adoption and NYCSF adoption, if you're already doing that and you're already measuring it on a regular basis and you have yourself a roadmap, you're probably in great shape already in at least on the essentials. You know, maybe there's some gaps on the enhance, but but again, taking a look at HICP and taking a look at NYCSF and really embracing those as the standards, I think, is again good advice for everyone. All right, so show me the money. If I do all this, what's it going to cost me? And is there any help? We're from the government. We're here to help, right? Let's find you.

Erik Decker: I don't work for the government. People always think that I do.

Ed Gaudet: I don't know. Neither do I. Neither do I.

Erik Decker: Yeah. So again, the strategy on this was a bit of taking a bite out of the meaningful use and what was successful with that. Again, we can argue there's elements of meaningful use that didn't work well. But the concept was right, which was, we want to get to better digitization of the EMRs. We want to get to, you know, if we have the if everything is digitized, we can improve our health outcomes. We can do all of this stuff, but it's got to start with getting to the adoption of the EHR. And in order to do that, you need to incentivize the industry to do that, to adopt, and so those that are adopting early will get the incentive, and those that are going to wait it out will eventually be disincentivized. And so you give them a ramp-up period. You give, you throw some incentive stimulus into the mix and then you end it with a, okay, it's time, you know, kind of kind of mindset. And by the way, this time horizon we're talking about here is very long. But the, in the proposed budget that went to Congress that still has not been approved. You know, so this is the White House budget that was submitted. There's a $1.3 billion of incentive stimulus for the industry to adopt the essentials and enhanced, specifically 800 million for the high-need hospitals like critical access hospitals, rural hospitals, those that are underwater to get the essentials adopted, and then 500 million for everybody for the enhanced side of the house. And it's a staggered sort of ramp-up period. This is the proposal is, and starting in FY '27 is when the incentivization starts, and then the, on the essentials, and then mandates will start in 2029. That's five years from now. So they are being very thoughtful that, five years is a long time, and, you know, this could all change again in five years. And this is not a statement of me saying, like, you have five years to do this, you should be doing this now because you have your own reasons to secure your business to do this work, and you should be doing it now. But what the disincentive will look like is in 2029, the basket update will be effectively nullified if you haven't done it. And what that means is every year, CMS produces it, updates its rates. And so due to inflation or something else, so say it's a 2% or 3% or 4% increase, they have upwards of removing that 2%, 3% or 4% from the reimbursement rate and critical access hospitals, the payment reduction of about 1%. It might not sound like a lot, but think about $100 million, on a $100 million payment, 1% is a million bucks, and that's a lot of money for these smaller organizations.

Ed Gaudet: Absolutely, all right. All right. So let's talk about how we get there. I love this slide because it really starts to define how to think about the roadmap for adoption.

Erik Decker: Yeah. So, and this is, again, you can argue about impact and effort. It's intended to be a framework to think about how you, to guide you. It's not intended to be the playbook that you use. In fact, I don't think we even released impact in an effort as part of the CPGs. This is just a thought, a thinking process that we had. So, but, you know, at the end of the day, this is going at, what are the ways that we're getting beat? Lo and behold, the top three are the three things that I just said. Social engineering is email security is going to help you on that. Not 100% protected, but it will help you on that, mitigate known vulnerabilities. That's already self-evident, and multi-factor authentication, self-evident. It's it helps protect against social engineering. This preparedness and and planning, you know, this is the, we want to prevent everything as much as we can, of course, but you have to have response actions and drilling those response actions and making like backups and all that kind of stuff that's inside the preparedness piece. And I'm not going to go through all of these, but, you know, the gist is where you have effort and impact like this can help if you haven't done any of these yet, you know, maybe, and you need help trying to figure out which one you should do, this can help you sort of guide accordingly.

Ed Gaudet: Yeah, great. In the same on the enhanced side as well, that's right. Any of these you want to call out or, you know?

Erik Decker: You know, I want to call out the top one, and this is actually was a big debate. You know, the top one is the EDR, effectively, and the EDR tools and the response actions associated to it. You really need to have EDR, and it's not in the essentials. I'll leave that to a beer conversation later. But the, if you get hit a couple of things, couple two points, actually. One, if you want to be insured, they're asking about EDR. And if you don't have EDR, you have a very high likelihood of not being insured. So that's a commercial pressure, a market pressure that is placed on us, not from the government. And two, if you do get hit and you don't have EDR, the first thing that happens is you deploy EDR.

Ed Gaudet: Right.

Erik Decker: So just deploy EDR.

Ed Gaudet: Get ahead of it, get ahead of it.

Erik Decker: Get ahead of it.

Ed Gaudet: Sage advice. Sage advice, all right.

Erik Decker: Yeah, anyways. Go ahead.

Ed Gaudet: Yeah, no, no, no. And, of course, you know, there's a ton of resources available. We're going to we're going to talk about some, on a couple of slides, moving forward. But but any of these, you want to call it obviously, you know, go to the HICP 405(d) website. There's plenty of tools that the team has built over the last few years. There's obviously the documentation, which is the playbook for good cyber hygiene, right? And we should all be doing it, and there are tools in the marketplace that can help you, manage the process of applying and adopting HICP and measuring it over time so you can take advantage of the public law 116 321 should you be under investigation. The landscape analysis is a great report. It's a great read, and there'll be, is there another one coming out, Erik?

Ed Gaudet: We're just starting the, getting the engines running on, starting to do that analysis again. You know, we had originally probably more, the eating more than we can consume kind of thing. Thought we would keep it up every year. It's hard to do that. So we're, yeah, we're getting through the organizational side of it, you know, the leadership who's going to run at this time, how that's going to play itself out. But you know, I, the goal, hopefully, we would have another one of these reports out by next year, and we would be able to see how things have changed. And that's really the big question always is you start, you get your baseline, and then you see how trends are forming, positive or negative.

Ed Gaudet: Right, right, absolutely. And then, you know, part and parcel with that is the benchmarking study that Censinet co-sponsors with class and the American Hospital Association and the SSC and others. And that's been a part of the data set that you had used for the landscape analysis and will continue, obviously, to use for the landscape analysis. So those are the resources.

Erik Decker: That's one thing I do want to call out. You know, for those on the call, we looked at investment in cyber as a component of small, medium and large. And this is what the benchmarking part of this is, so both on the monetary side and the investment side and then the staffing side, like what does the staffing ratios look like? And we got all of this information. I think it was like 60 people, 60 health systems that did that.

Ed Gaudet: Well, now there's over 100. But yeah, there's over 158. When we did the first, yeah, yeah.

Erik Decker: And so, you know, and we, we did a box and whisker, you know, like, what's the bottom 25, upper 70, upper 25 look like middle 50. And it's really insightful to see like where you're where you're at in your journey. And if you're under-invested you, it's a potential thing to point to, you know, back to your organization to say, look, look, here's where the rest of the industry is. And by the way, I think, in general, we don't invest enough in healthcare cyber. So we're kind of already investing at a lower level. So if you're below the lower level then then, you know, maybe that'll that'll help you out. For those that do have good investment, it can be a little bit of a harder conversation, you know, because you don't, it's not regression to the norm that we really want to get to regression to medium, but it's good data.

Ed Gaudet: Excellent. And it's available, and of course, you know, this is just a plug for Censinet as you start your journey down your compliance program for the CPGs, we're here to help you out. We can help you manage them, take the data that you already have if you already are a customer in the system, and we can map it automatically to your where you are in your CPG journey today. So that is available today in the product in the sense that at risk ops platform. And just another note that for folks that are just starting their journey and maybe want to start with HICP, as we talked about earlier, the AHA and Censinet work together to provide HICP support at no cost to the marketplace. So if you're a small organization and you want to see where you are relative to HICP, you know, reach out to Censinet, and you can get started today at no cost, and that's going to be available forever, so. Well, you don't, you don't get in. And then, we charge you, you'll have access to the HICP module forever based on the AHA partnership we have. All right. And, of course, as Erik talked about, that data is leverageable across the peer cohort. So you can see where you stand relative to your peers. You can obviously do that with HICP.

Ed Gaudet (cont'd): You can do that with CSF coverage, and now you can do it with CPGs as well. So you can really get a sense for where your gaps are organizationally from a resource and investment perspective where your coverage is across those three, you know, the two recognized security practices and obviously the CPGs that are required standards. And, or do we call them standards, by the way?

Erik Decker: The CPGs?

Ed Gaudet: Yeah.

Erik Decker: No, no.

Ed Gaudet: I think they're I think they're becoming there's this notion of a de facto standard. I think it's becoming a de facto standard, right? But anyway, so that's all available as well, and can allow you to start to create your own baseline and to measure that with a peer group, as you had done your journey. Alright. And we are at the Q&A point. So, we've got some in actually in the.

Saul Marquez: We do have some questions.

Ed Gaudet: Yeah, Q&A channels, so I can see it. I'll just go ahead and.

Saul Marquez: Sounds good.

Ed Gaudet: Yeah, read these. So Erik, this one basically says, doesn't feel that HICP is getting the attention it deserves based on its power. What marketing initiatives and programs are you all working on to further spread outreach and awareness?

Erik Decker: Yeah, that's a great question. You know, I'll say. I wish I had the stats at my fingertips, from when we launched HICP in 2018, and we weren't even tracking engagement to the new website that was launched. And I think within like the first month of the new website, it was something like 400,000 hits or something along those lines to where we are today, which is 3 million views. I mean, that's a great, that's a great trend.

Erik Decker (cont'd): The challenge that I think is, you know, and I still go to conferences and things, and I do talks, and I'll say, who's heard of HICP? And, you know, I have not yet gone to one of those things, and the entire room has raised their hand. You know, like, if you say, who's heard of HIPAA? Like everybody's going to raise their hand. So it's not, it's, but I will also say it's not like the entire room is silent and nobody's raising their hand. So we, it's like 20%, 30% of the people, generally speaking, that know about it, and that's all completely dependent on the form that you're in as well. So we do have this, I will say this. So there's, there's a whole machine that is run out of HHS, the 4 or 5 program within HHS. And they take the content that we've cleared, that we've developed and cleared through HHS, and they are producing all kinds of stuff as a result of that. So they're on social media. They're doing there's like this myth versus fact. There's, that looks risky, like little vignettes, you know, like little, little nuance things. Yeah, there's a new cyber pulse that was just released that was actually in partnership with the industry where they were like, check your cyber pulse. And how does one check your cyber pulse? And it's all like different ways of trying to get at this core under an underlying problem or underlying symptom at the end of the day. We also have ambassadors. Ed, you're an ambassador.

Ed Gaudet: I am an ambassador.

Erik Decker: So these are people who have volunteered to, like, spread and evangelize and prophesize, you know, the work. We've we've hit our community fairly well, IT and cyber in healthcare. I think where we need we need continued market penetration are, you know, the clinical side of the house, the AMA's, the, there's a thing that one of our ambassadors just did Donna Grindle just did up here in Chicago this last weekend. There's an ortho meeting, and it was just all surgeons, you know? Orthoscopic surgeons, and she was there talking about HICP. And I think that's the kind of thing that we need is to get out of the IT and into more of the business and clinical and financial side of the house to get more traction. I will say, when HHS did mass release of stuff, it garnered a lot of interest. I think we're going to see more of that as well as it gets more and more embedded in stuff like the CPGs, like the law 116 321, at the end of this year there, OCR is reopening the security rule for the first time in 20 years, and they're going to be doing a notice of proposed rulemaking, and that's going to be one of the avenues that they use for mathere's other opportunities. And I would say, like everybody on this on this webinar, if you believe in this, you should be spreading the word, you know, to get it out.

Ed Gaudet: That's a great point. Everyone can be an ambassador. Reach out to the 405(d), there's ways to get involved. Please get involved. We need the help. All right, so, second question: part of the effort you just explained, Erik, what is the place of AI? In other words, I'm glad we got the AI question out of the way. In other words, are those efforts flexible and adaptable? Yeah, to this era of emerging technologies such as AI.

Erik Decker: You know, great question. And, you know, I think AI, it warrants its own special place. You know, what we're talking about here are is cyber hygiene, its basics. And AI is a different beast entirely with different challenges and different issues. And so, I don't think like a CPG around AI or a HICP module around AI is the right path per se, because it's again, we're talking about resilience and hygiene, you know, versus AI challenges. Now, I don't want to be myopic here, you know, so I can be used as a way of like making social engineering more effective. We've already seen that happening, or you know, there's, there, boy, there were some like, horrific deepfake things that I've, I've heard about, like people getting on a Zoom call, and it's all deepfakes, and it's all voice deepfakes, where they were tricking the CFO into a fraud, fraudulent transaction. And it was like me and you, editor, on a call, and it wasn't you and I on a call, you know, and it was. That's scary. So I think, you know, we, we're just on the cusp of like, what the new frontier of AI challenges are going to be. There is an AI task group that has stood up as part of the critical infrastructure partnership, and I think that needs its own cyber work as well as like ethical and responsible use of AI. It's a whole beast in its own right.

Ed Gaudet: Yeah, the Healthcare Sector Coordinating Council has a paper, yeah. It's actually a year old, believe it or not. Yeah, I went back and looked at it. It's still fairly relevant. There's still topics in there. Take a look at that. To Erik's point, it is a, you know, a large, large, evolving beast that is getting a lot of heat and light and attention. However, when you think about even the essentials and take number ten, the, my favorite one, the third party, right? You at least have to get quickly educated on third parties and how they're going to be bringing AI into your health system. There's going to they're going to be through new contracts and relationships. You have. So you have to think about how do you assess the risk associated with AI that's in that context. There's also those that you already have relationships with. This is even the scarier point, in my opinion, where they're bringing it in as part of an update. And so you may not even have done your initial assessment on these folks. And now they're bringing in AI, which can cause, you know, potential risks to, you know, to data and to access.

Ed Gaudet (cont'd): So I guess the advice is, get on top of AI as quickly as possible and look at it across the essentials at a minimum, as you start to parse how you're going to approach it longer term. All right, so next question. My IT director tells me that even if we have are EDR, it requires 24/7 eyes on glass to make such, to make sure threats are reviewed in real time. How would this be realistic for smaller organizations?

Erik Decker: So your IT director is correct? EDR is a I mean, it has some preventative capabilities, but it is largely a investigative tool that lets you know where people are moving around laterally and how that's happening. So this is definitely a conundrum, definitely a challenge in this space. There's not enough people, there's not enough cyber people to do the work for everybody, and in the smaller side organizations, you know, the chances of you insourcing a SoC are very small. The chance of you actually even having a cyber person at all is very small. Even having the chance of you having an IT person is very small, or maybe you have two or 3 or 4 IT people. So this is where your service, your managed service, security service vendors can assist. I would say that it's not a panacea. You can't just slap it in, get a contract, and then say, hey, we're good, because so and so is watching the, you know, watching the house. You do have to manage them as they're doing that, there are really good players in the space, and there are really not great players in the space, just like with everything in IT, you know? So, but getting to that situational awareness, like, even if you don't have a SIM or like a SoC or anything like that, you know, an EDR and XDR, those are like the first cut, you know, of monitoring that people are doing now, and I think it's a great first step.

Ed Gaudet: Great, great, excellent.

Erik Decker: And by the way, some of the EDR tools that you use already come with monitoring from the company that has the tool and depending on who you're using. So that's another option too.

Ed Gaudet: Yeah, yeah, and as you mentioned the, a managed service provider can also help, you know, with the low-cost option to manage that for you. All right, so let's, this one I think this one is more of a statement. But question is, will voluntary compliance ever get the job done in terms of security and healthcare? When will we accept that unfunded mandates are ineffective and we need laws and regulations? How do we drive that?

Erik Decker: So I'm going to ask this question. Has voluntary adoption of cybersecurity controls over the last 20 years got the job done? I would say no. It has not, because we are facing every year more and more damage and more and more impact, and you know, the comment about unfunded mandates, that's why there is a white House budget proposal. That's why there's $1.3 billion. That's why there's a two-year ramp-up for essentials, and then another two-year ramp-up for enhanced. At the end of the day, we all have a job to do here. And, you know, we can argue that, you know, the government is inappropriate or whatever, or, you know, we can rally against or rail against that, but it's not solving problems. And I think that the way they approach this, they listen to us, and they actually took exactly what we said, which was incentivize, give us a ramp-up period. Do not slam this down. Do not come in and say, you got to do this and there's no money for it. You got to do it in a year because you're going to have a riot on your hands if you do that. But if you have a five year period of time, you know, in order to get this squared away, you have ample time in order to, to, to get there. And honestly, you should be wanting to do this anyways because if you will get hit, if you don't do these things, it's just, it's inevitable.

Ed Gaudet: And it's a good reflection of the partnership to the private-public partnership. Like you said, they did work with, you know, the industry too, they just didn't come out with, you know, the, you know, the tomes from the Mount.

Erik Decker: And on the point of, I see, as I'm reading this a little bit more, the needs for law, regulation, how do we drive that outside of, like, voluntary compliance? That's actually what the reopening of the security rule is about. And as well, they're looking at CMS is looking at its enforcement actions under conditions of participation. So accreditation, you know, you know, everybody who participates in the JCO and DMV, you know, accreditation processes and the tracers there. You're going to start seeing cyber as one of those tracers. So that will also drive it. And I also mentioned earlier anyways, but the market pressures from cyber insurance, you're just not going to be able to get cyber insurance if you don't do these things, if you don't even do the five things. And so, like, that's another pressure. That's just not, it's outside the organization. So those are all ways to help get us into a better place.

Ed Gaudet: Yeah, excellent. And the next question is, what does the partnership you mentioned for AHA members? Again, it's free access to the ability to, for you to start managing your HICP adoption through Censinet.

Ed Gaudet (cont'd): And if you're interested, you can just shoot me an email, it's EdGaudet@Censinet.com, or just reach out to Info@Censinet.com for more information there. Next question: how should smaller, resource-constrained teams prioritize adoption efforts both in focus area and product evaluation? A great question.

Erik Decker: So I will go back to that slide that showed impact and effort and look at do a quick little gap analysis. You know what of those things do you already have in place? Do you feel comfortable with or what do you not at all have in place and where you have a big gap, especially if it has an the impact of what that means is like, what's your impact to cyber resilience going to look like? The higher the impact, obviously, the better. So that could be a place to get into prioritization. And then, as far as the evaluation of the product itself, you know, we definitely do not do that. We don't touch that. We have to stay away from that. We have to be vendor-agnostic. So there's no competitive edges here or anything. But, you know, I would, I would, my recommendation would be, go to your associations that you're a part of and ask those questions, go to your networks or peer communities and ask those questions. Go to your people. If you have people that are subject matter experts and, you know, get their opinion. You can obviously talk to the vendors themselves. You're going to get a biased opinion when you do that, and, you know, and just kind of vet it out that way. And really look at what, look at the CPG outcome statement and look at what it is that is trying to be accomplished. And just make sure that that product can achieve that. That's that would be another thing that I would throw in there because I, I think I've already seen some folks kind of glamouring into this and saying, we can do this, this thing over here. But maybe, maybe they do. Maybe they overlap great 100%, maybe they overlap only like 50%. So you have you have some due diligence you got to do.

Ed Gaudet: Excellent, excellent. So this question basically talks about securing digital assets and getting CEOs and boards more invested in helping out. And so, you know, how do we do that as an industry? How do we get the boards to be more accountable for cybersecurity?

Erik Decker: So there's a really good book. It's actually kind of a book. It's 100 and some pages, and it's freely available. The National Association for Corporate Directors, NACD, has, just last year, they updated a Cyber Risk Advisory Toolkit, and they talk about six principles of what governance of cybersecurity looks like.

Erik Decker (cont'd): And this is not stuff that the CISO should be doing or the cyber team should be doing, it's stuff that the board, the committees of the board with management, you know, should be looking at and doing. I would give that a read. It's a really, really good book. It has a lot of good questions inside of it. And if if you're in an organization that is not really being forward-thinking about this, the first thing that I would do establish governance. And that in that organization, you know, where you garner up key members, not IT people, business people to take on the challenge of, like, owning policy, owning the risk posture in the organization, owning decisions on risk like risk appetite and risk tolerance types of decisions, and chair that group, again, not the CISO, but somebody else in the business, you know, hopefully like an executive leader or somebody along those lines, if you can get them and then start meeting regularly and start discussing these things. You'll, that is a formal way to kind of get to an organic change. But once you charter something like that, a governing body, and you start having an ongoing dialogue, and then you start talking about it at the board level and so forth, it starts to get its own momentum, and now there's a lot of work to do on this. This is why the CPGs will never answer all. Notice I, governance is not in the CPGs, but the, you know, like that will help you get momentum to getting a program established to getting some funding established and getting a cadence around where you can have a dialogue around these challenges and get some decisions, and it takes it out of the hands of the cyber team when you do it that way, which is a good thing because you, then the business is actually there with you, partnering with you and owning it with you.

Ed Gaudet: Yeah. And there is some work on the, at the SEC level for publicly held organizations where they're trying to actually mandate more board oversight and board accountability. So, I suspect that'll, you know, this year, we'll start to see some things fall out of that work. Let's see, question about CPGs and business associates. Are they, do business associates have to have to comply with the CPGs?

Erik Decker: Could you go back to the diagram? The second slide. The ecosystem.

Ed Gaudet: Oh, okay.

Erik Decker: So, first of all, CPGs are voluntary right now. And, you know, we're we talk about mandates like the mandating side of this is rulemaking. Rulemaking happens within the federal government.

Erik Decker (cont'd): This is a case where you could actually speak with your congressmen, senators, and give them your perspective. If you have a government affairs office inside your organization, I would encourage you to do that. You can also work with your associations because your associations have the ability to provide this voice. Here's what I'm going to say. An ecosystem doesn't care if you're a covered entity or a business associate. An ecosystem is an ecosystem. And when you are connected, you're connected. And so, if we're going to get better at this and we're going to resist and to do what Chris Inglis says, which is you have to beat all of us to beat one of us, all of us have to be doing at least the basics in order for this to work. So my personal opinion is, yes, the business associates should adopt, and they should be they should be connected or if they're going to be connected. Or maybe, you know, maybe I can force that on them by the kind of connectivity, although that puts the monkey on my back then to argue. And that's just more arguing, which I don't think helps anything, but I frankly believe that we all have to do these basic things, and we have to make it harder for the bad actors to do what they do. They are going to do what they do. There's no stopping them or there's no stopping their intention. I should say not, no stopping them. But we need to make it as expensive as possible for them to do what they do, because that's what, that's the game. It's an economic. When we're talking about extortion, we're talking about disruption. It's an economics game, and we want their return on investment to be very low. So you, we have to build our defenses to do that.

Ed Gaudet: Excellent, excellent. So let's end on that note. What a terrific webinar today, Erik. And thanks, everyone, for your questions. I mean, this is I don't think we've had this many questions on the webinar before, so, and people are still still here with us, so I guess it's, that's a good sign. So people enjoyed the topic. And, thank you, Erik, for your time and your insight on this topic.

Erik Decker: Thank you.

Censinet RiskOps™ Demo Request

Do you want to revolutionize the way your healthcare organization manages third-party and enterprise risk while also saving time, money, and increasing data security? It's time for RiskOps.

SCHEDULE

www.Censinet.com