Webinar

Risky Business - A Webinar for Cyber Risk Practitioners - Part 4: Ain't no Mountain High Enough

Saul Marquez: Hello everyone, and welcome to the Risky Business webinar series. We want to thank you for making the time to attend today's session. This is the fourth and last of four webinars, all dedicated to helping risk and security professionals like you. Today's focus will be on why leading CISOs are building GRC programs, secrets to long-term GRC success, and how to use peer benchmarking to elevate GRC performance. Today's webinar hosts will be Chris Logan, senior vice president and chief security officer at Censinet, and Matt Christensen, senior director of governance, risk, and compliance at Intermountain Health. Just as a reminder, today's webinar is being recorded. We invite you to use the Q&A feature on your Zoom participant screen to submit questions as they come up for you, and we're going to address them at the end of today's webinar. Both the slides and the video recording will be made available to you after the webinar via email. And if you wish to receive CEU credits for today's webinar, just reply to that email with the slides and webinar recording so we can get those credits to you promptly. Looking forward to having you all on today's webinar. I want to welcome you. And now I'd like to turn it over to Matt and Chris for today's program. Welcome, guys.

Chris Logan: Thanks, Saul, I appreciate it. And boy are we excited. What a topic we have for you today. Talking about governance, risk and compliance in your healthcare organization and really how it can be a game changer for your organization to truly understand its enterprise risk appetite for risk. So I'm really excited to dive into this topic today. I have a great co-host who's going to share his experience. So let's start by just introducing ourselves. Right. So welcome. I'm Chris Logan, senior vice president and chief security officer here at Censinet. I've been in the healthcare industry for way too long. At this point. I've sat on the other side of the desk as a healthcare CISO for a number of years. My journey to the other side, to provide my skills and talents, to help really satisfy the needs from the ecosystem of partners that are helping deliver products and services into your healthcare delivery organizations. And enough about me. You've seen me. If you've been on this, this webinar series before. So you're going to get much more of me as we go along. But let me pause and welcome Matt to come in. Matt, please share with us a little bit about your background and who you are.

Matt Christensen: I will do. Thanks so much, Saul. Thanks, Chris. So my name is Matt Christiansen. Um, I'm the senior director of GRC, as was previously mentioned. Um, I don't have near the experience in healthcare that Chris does. I'm about ten years now in healthcare and then just over 15 in cyber itself. So I got my start in, uh, in the largest call center in the world. We supported 125,000 employees and a team of five. So it was we were busy, I think is how I would say that, and then just worked in different roles within risk, internal audit, and cyber. So glad to be here. And while while we're waiting for it looks like a few more of you will join; please drop in the chat where you're calling in from. I always love seeing where people are actually listening to us.

Chris Logan: And Matt, give yourself some credit. Just because I have a lot more battle scars from being in the healthcare industry, it doesn't mean we haven't shared the same, uh, same landscape, my friend. Right. Just in different shapes. That's right. Just that new thing. So what is the Risky Business webinar series? This has been a journey that you've taken with us, and I greatly appreciate everybody's participation up until this point. We really started this thing back in June. Looking at what are some of those best practices for managing third-party, managing risk assessments in your organization? Create efficiency and effectiveness. And then we turned it into not just worrying about that digital landscape that's coming in from the ID department. What about the rest of the enterprise?

Chris Logan (cont'd): So when we talked in July about All Together Now, it was really looking at cyber risk as it's pervasive across your entire operating environment, really going into places that it's never been before and how to protect patients from cyber attacks and those risks that are constantly being pervasive. You know, last month we had the great opportunity to have a wonderful discussion about one, how to just advance your cybersecurity career but also learning lessons from a current sense of customers and provider about how they're using third-party risk to really influence and engage training that next level assessor within their organization to work at the top of the license. So now we're winding this thing down. This is four of four.

Chris Logan: This is you know, big expectations here Matt. Right. Because ain't no mountain high enough. How do we take all that we've learned up to this point, all that we've explored, and really tie it into what governance, risk, and compliance mean for our organizations and how to use that to more effectively display or just inform and educate people about the risk that your organizations are undertaking. Now, with that said, the landscapes really significantly changed over the past 1015 years. If you think about cyber in its role today, it's really about patient safety risk. The digitization efforts that we've gone through and how pervasive it is across our organization has really created this confluence of forces that really compounds risk to patient care across all of healthcare. Just as a background, one of the things that we've seen over the course of the last few years is that ransomware attacks are growing in frequency, and they're getting really vicious, right? So it's not just about a smash-and-grab locking up your data. It's really about making it truly unavailable to impact patient care. And the industry is facing some shortages here. And it should come as no surprise to anybody on this webinar that there truly is a workforce shortage when it comes to cyber. Healthcare is not the only one suffering from that. It's all industries, but with the specialized knowledge and the complexity of the environments that we operate in, it's really important to have cyber at the forefront and really figure out how we address that shortage.

Chris Logan: And what's also taking shape is that we're seeing healthcare being delivered well beyond the four walls of the hospital. Digital is here to stay. It's not going anywhere. The cat's out of the bag, as they say, right? And we're going to continue to look at digital to drive better outcomes for patients. Drive better. Um, just service line delivery, give people what they need for care and meet them where they are in their care journey.

Chris Logan (cont'd): And what's really happening when you think about digital and expanding that attack surface is it's fueling this explosion in third party enterprise risks. So, really understanding what this means to your organization. Now what we're also seeing is that it's not just one silo. It's pervasive across the enterprise. So, if I look at cyber risk teams or cybersecurity teams in healthcare, you're being asked to do more with less. So you're facing these superhuman demands, right? Third-party risk management is only escalating that because now you have to look beyond what you're inside the four walls of. How are other people operating and using my information? So when you see that the shortage of workers is there, you're really seeing demand outstrip supply. You're now looking or being pressed to do more with less and understand more about the environment beyond the walls of your hospital so that you can operate safely inside. Think about the complexity.

Chris Logan: So again, that digitization, you now have to capture and assess significantly more data points. And just an example, things like AI and ML that's creeping into how healthcare operations are providing care services or even something as simple as move it for an example. Right. A small software package that has a significant impact when it comes time for patient confidentiality. More importantly, not only being able to look at more, but you got to do it in manual fashion. So how do you monitor in real-time? Well, managing this here creates an ever-expanding landscape of enterprise risk in the way of things like clinical risk, operational risk, financial risk, and then others. I can't stress this enough. If you think about that landscape, tying in governance, risk, and compliance into these areas as focus points becomes a crucial component of your security program. And educating those folks on the other side of the fence. So why GRC? What is GRC? I can tell you what I think it is, but what I'm going to do is I'm going to pause, and I'm going to throw the baton over to Matt here because this is his bread and butter. This is his baby. This is what he knows inside and out. So Matt, please share with us your vision. What is GRC? What's an effective GRC program, and what are those things we should be concerned about when we think about governance, risk, and compliance programs in healthcare?

Matt Christensen: Yeah, yeah. Great. Great. Intro. I related with much of what you said, and I think specifically, as you were talking about ransomware and just how fast that is growing, the one thing that is positive about ransomware is if there is something, and that is the awareness on the caregiver side. Now, so specifically in healthcare, you know, you used to be able to talk about you would you could bring up things like, oh, hey, what do you do?

Matt Christensen (cont'd): Like if you're seen as a patient, right? And you just have that small talk, they say, well, what do you do? I work in cyber. And then you start geeking out on them and they just kind of tune it out. Well, now when you say, well, I work in cyber, you know, we help prevent ransomware. Then it's like, oh yeah, I know what ransomware is. And then you can actually have dialogue. So I think that part's great. The easiest way I would summarize what GRC is. It's all about creating culture within security as a culture. I mean, that's the easiest way to just boil everything down. And what is what is GRC? And that is helping create a culture of security in an organization. You know, I think too often we have practitioners where when they're presented with a risk, they'll just go straight to what we have to put something in place, a lock on the door, a bolt on the window. You know, um, security guards in the front. And I think too often we've just had this culture within the practice to just say, if there's a risk, then we mitigate it when really there's multiple ways you can manage risk.

Matt Christensen: You know, you can avoid it and just not do it entirely. You can transfer it, you can share it, you can mitigate it. There's different ways that you can do it. And I that's where I see us going. NextGen is just re-educating folks. And in many times the people that need the re-education is our own team, our own, you know, cyber shop itself of saying, yes, there's risk, but it's within the bounds that our executives and our board have set. So I think that's, um, one key important point to remember is just that cyber doesn't get to determine risk. Um, it's our job to to put in front of our executive team, our board of directors, the risks at hand, and then they get to set those tolerance levels. Um, and we're going to get into that, you know, in in future slides. But yeah, I love that cyber really can help create that culture. Um, we're not a know shop and we and we can't be. Um, I think when you, when you focus on hearing a risk at hand or one is presented like move IT you want to just, I don't know, some of us just say no. We just say like we can't accept that risk, right? Or the business wants to be able to deploy in a new cloud environment that you haven't been in before. And it's not about saying no, it's about what do you want? And how can we how can we meet that need? So that's a big part of GRC.

Chris Logan: No, that's fantastic. And we've had this conversation a couple of times. We've talked about this at length. I think some of the key things that you've brought out in those conversations, although it may not have been direct, it may have actually been, you know, on the periphery is that risk across Organizations is unique, so my health system may be performing the same function as yours, just in a different form or fashion.

Chris Logan (cont'd): I need to understand why that risk is really unique to my organization. So I'm not the know shop. I'm the yeah, we achieve this, you know, ask the why question and get to the right answer. And the idea that nothing is perfect. I want to stress this as well to everybody that's in attendance. There's no silver bullet for security in general. Um, if there was, we wouldn't be having these conversations. Right? The idea at the end of the day is that there is no perfect. We strive for perfection, and we continue to learn as we fail, as long as we fail fast and we fail forward. Right? Because at the end of the day, we're going to have those shortcomings. Identifying those shortcomings is the key though. So I want to I'm going to jump. What do you got? I see you got something. Yeah.

Matt Christensen: No, it's fine if we need to move along. I think just to reinstate what you were going to say. I mean, when it's really easy to want to just say, okay, business, you tell us what the risk is, and then we'll work to that. And it's not like that. I've never been in an organization where, you know, you'll have a board of directors and executive committee all come together and define what cyber risk is, and then hand that back to you and say, now go protect it. It goes the other way around. I think it's just understanding that accountability. It's our job as practitioners to provide them with good information, with the ability to say, these are things you should be concerned about, not the gnat's eyelash, Right? it's the things big things like this will impact patient care. Those are the things that the board wants to know. And and so yeah. And then we just, I just see it too much where everyone's like, all right, you just tell us what it is, and then we'll work to do that. I'm like, no, that's not a good partnership.

Chris Logan: I agree, and we're going to dive into this a little more.

Matt Christensen: Yeah we will.

Chris Logan: There's a subsequent slide that's going to speak to this concept or idea of themes that you're alluding to, right? So we're going to frame out a couple of topic areas. Right. And this is just used as a guide for us. We do have slides to back us up to create some talking points and some dialogue, but we're going to really focus on these six areas to really define what next-gen GR Success Pro program success could look like to an organization. So let's do that. Let's hop right into this first one, defining the overall enterprise risk appetite.

Chris Logan (cont'd): In your experience, in your travels, the work that you're doing today, how do you help your organization from an enterprise perspective, really understand what that risk appetite should or could be?

Matt Christensen: Yeah. It's not it's a great question. It's not about, you know, you've got this Windows 2008 server, you know, that has 18 different patches that haven't been applied. It's not that if you go to that level it just flies over the board. They don't understand. And you likely won't get the support that you're seeking and should have. But instead, you know, it's bringing it to that. If you're in healthcare, it's bringing it to the level of the clinician and saying, you know, if we don't do this, then this is the applications that will impact. You won't be able to take x-rays; you won't be able to, you know, to do imaging, whatever the case may be. It's it's getting to that level. So I think that would be the first thing is just saying, you know, and we and there's that I think we started with cyber safety as patient safety and patient safety. Cyber safety right. So I think just moving forward with putting terminology that can be understood, that isn't fear, uncertainty, and doubt, but it's palpable. You know, it's terminology that that hits home and specifically at a bedside or surgery site or an Ed or whatever the case may be. Um, and again, this changes as your organization changes.

Matt Christensen: You know, 3 or 4 years ago, Intermountain Health was a mostly Utah-based health system. And now we're in seven states and we have 300 over 300 clinics. And, um, so absolutely, our appetite and our tolerance levels have changed since our strategy has changed as well. So that would be one I don't want to say advice because that makes it seem like I know it all, but that would be perhaps a takeaway for the audience to go back and say, when was the last time we defined risk tolerance and appetite? You know, even as a team, and then brought that up to the executive level and had them review and agree to it, and then how often are we revisiting it? You know, there's a good reason that you increase the speed limit on certain streets when you can prove that it doesn't necessarily decrease safety. And you've got to do that at the board level, it's continually revisiting those themes, reaffirming that what we believe is the highest risk and what they, you know, have confirmed then then we're all on the same page. But you've got to revisit that. You can't just set it and forget it.

Chris Logan: Well, it's an interesting concept in this dynamic that we, as human beings, as individuals, deal with risk decisions on a daily basis. I mean, just even getting up in the morning is a risky decision. Sometimes it depends on where you are. So, you know, and I think about how you're defining these key risk themes. How do you ensure that you're managing those key risk themes? And you're educating folks consistently and constantly to make sure that they understand the risk that they're willing to accept?

Matt Christensen: Yeah, yeah, they have to be a theme. They can't be. What are the specific threats? What are the specific risks? You know, like we talked about the gnat's eyelash. It can't be that it has to be themed. And I believe there's a future slide on that. But you know, we'll probably get to it. But those themes really focus on at least in our strategy around always patient safety, always. Right. And then you know, you've got safeguarding financial assets and privacy and security. And our fourth theme really is around growth and complexity. So you have different risks, you know, at the highest level, that first tier, as we like to call them, the board should know about. And there should be an easy way for them to understand, to say, yeah, we're within those tolerance levels, we're okay with that. And they should know and very easily understand when we're moving outside of those tolerance levels. And I think that's where, you know, that's where the CISO and the CIO really play a big role in, in putting it in language that they can understand, in metrics that they can understand where it's not technical, you know, jargon. It's not. You don't inform them with as I said, cvss scores and certain vulnerability levels. And I don't even know if it's so much as a stoplight. I mean, it's we'll get to it. But the more you can simplify GRC, the more effective your program will be.

Chris Logan: Yeah. And we're going to talk about that in the very next slide. But there's one other thing I wanted to point out here. If you look at the left-hand side of the slide, it's not just one icon.

Matt Christensen: Yeah.

Chris Logan: It has to be an enterprise battle. Everybody has to be involved in this process because if you don't and you do it in a silo, the chance that something could go wrong there is exponentially higher.

Matt Christensen: And what I love about that is Chris has been cyber for so many years. You know, you've been in the game long enough. We're no longer an afterthought. I think we're well past that. It took a quarter of a century, but we're past that now. But we're now at the table with HR, with legal, with compliance with other operational leaders. Right. And it doesn't take much. In fact, one of the best ways that you can get buy-in in some of these other areas is to run a tabletop exercise. It's to basically say, okay, we just had a ransomware and we now no longer have HVAC systems. How do we, you know, what's our strategy? And you know, what's our playbook? How do we actually get continuity of services after that? And so I love I love that we're a component. We're within that spoke. Right. We're not the spare tire that's often forgotten about and neglected under the car, but we're core to the machine of all risk in any organization.

Chris Logan: I love it, I love it. Let's jump forward. What about those cores?

Matt Christensen: There they are.

Chris Logan: This is the thing we were lining. We teed this thing up so perfectly, I think. Right. So what what are these core risk themes? What are you seeing? What's your guidance here? I know you started to share some of this. Yeah, I went to a deeper level.

Matt Christensen: Yeah. You bet. So first and foremost, patient safety for Intermountain Health is everything. Um, and think about that. You it doesn't you don't have to, you know, contemplate too deeply or very long to relate to this. Uh, most of us within the last three months have been in and seeing a physician or, within the last three years, have had either a minor or major surgery. And don't quote me on those statistics, but we're in the building frequently as a patient if nonetheless, we should be there annually at least. And if you think about it.

Chris Logan: At least once a year, please.

Matt Christensen: Just once a year. All right. Well, folks, you and I have. Yeah, maybe that's another topic we should have. I'm a frequent flyer, so we'll just say, um, you know, but as a patient, think about systems that are relied upon for them to give good care to you. You know, vital systems, your, your electronic health record, um, if you're if you're having procedures done I mean, it's it's everything from anesthesiology to imaging to, you know, everything through your post-op.

Chris Logan (cont'd): So having the ability to collaborate across the enterprise and really start to think about who owns what piece of this puzzle ensures that we're one meeting the measure of what we need to do from compliance hygiene and a framework perspective, but also it saves us time. It gives greater visibility and overview and allows the right person to effectively mitigate and manage those risks that your enterprises are seeing.

Phillip Robitzsch: Absolutely. And to piggyback onto that as well, before we jump to the next one, I've encountered that many times in my in the past three and a half years that I've been conducting risk assessments where I had to go on internal calls or other calls like, and just, you know, get this information that I need. But now with this automation included here in the platform, it's a simple share. With one click, they can provide me the information I need, and there's no need to find a time that works for everyone. Schedule a meeting Clarify everything. Go back and make those changes. Um, so as as Chris said, a huge time saver here as well.

Chris Logan: Yeah. And again, these are building blocks, right? So I think about the maturity aspect of any organization. You have to build upon these steps, right? To really get people involved in the enterprise risk that's taking place, really get that purview and that visibility seen across the entire enterprise. That's why it's so important as we focused on those first front areas, is that getting the house in order now, expanding it out to a wider breadth and depth of people really starts to solve the problem. So if we're automating those risks and holding people accountable for it and getting them involved, that now gives us the opportunity to branch. So when you think about risk from an enterprise perspective, and I talked about digital before, how it's so pervasive across your organization. What about non-technical vendors. Right. I'm really starting to think about this from the lens of, yes, digital is Digital here.? They're part of the supply chain. What about the remaining factors of the supply chain that we have to start addressing? And it should be no surprise to anybody. The largest breaches that we saw in the past two years up to this point have been supply chain vendors. It was not IT-specific vendors, printing and mailing vendors, and a dental benefits manager. Yeah, there's some components of data exchange that take place there. But now's the time as you grow that program and think about it from an enterprise perspective, it's not just cyber that's the problem. How do we get into the non-technical side of the organization and really think about strengthening the supply chain? It can only be done once we start to automate those findings and get the subject matter experts involved.

Matt Christensen (cont'd): All of that can be impacted directly through, you know, a material cyber event. Ransomware rarely will take out a single computer. And you don't just turn it off and go stand up a new computer or you move to the next workstation. Um, the way that it spreads. So we always start with patient safety. In fact, I've never once been in a meeting where we haven't started that conversation with, is there a way that this can, you know, negatively impact patient care, especially as we're doing risk reviews, as we're doing, um, you know, assessments on new things? That's always our first question: could this negatively impact patient care? And if it does, then guess what that does to our appetite and to our tolerance level totally shifts them. Yeah. These other themes that we've got listed there and we don't have time to deep dive into all of them.

Matt Christensen: But really, it's how we keep the business running. How do we maintain the privacy and confidentiality of all of our patients? And in our case at Intermountain Health, we're an integrated system. So we have an insurance component as well. So our patients and members safety you know their information safe. And then as organizations grow, you know, that landscape, the technological landscape changes. You introduce new networks into your environment, new cloud environments. You need to connect bridge A to bridge B with a million APIs. I mean, there are a million ways that you can introduce new risks into an organization when you are growing, and it is part of your core strategy. And the,n of course, safeguarding financial assets. You don't have money. You can't run a business. So those are the main ones. Then, really, what I wanted to focus on here is just that that's the level that you would focus on the board. That's the areas you would focus in and say to our board, to our executives, um, finding a way to, to give them a scoring component, you know, if that's a stoplight, a red, yellow, green type thing or a zero through ten, but that's the level you need to be able to introduce risk to the board as to how we're doing, staying within those safeguards that we've established.

Matt Christensen: The minute you go deeper than that, I think you lose credibility, you lose attention. And then that next layer down. We often refer to these risk statements as tier two. So that second layer is down. So if you think of ransomware or, you know, a DDoS or malware, um, any of those threats that you often hear about or experience, depending on how large your system is or your threat profile, that that's the statements that then can roll up to these main risk themes. So you might have ransomware roll up to multiple ransomware will impact patient safety. No question. Um, it does often, uh, include, you know, a potential disclosure of patient information.

Matt Christensen (cont'd): Um, and then you can just follow those themes down. However, not all risk statements will roll up and go to the board level. Again, you want you want to give them that enterprise perspective. Um, and then if at all possible, depending on the size of the organization, you may want to break it out into certain regions. So you can still show the board, you know like we're showing a four out of 5 in 1 of those, right?

Matt Christensen: Well, then what's the where are we, not five out of five? And then you can drill down into the specific, you know, regional area where you may not quite have the same level of security that you do across the enterprise. Then that third layer is really the the tactical gets that we need to patch these Windows devices or these, you know, Linux devices, um, need to be patched, whatever the case may be, that that's where you really get to that, um, that third layer down, these are the known risks. These are the that's where you typically will see your action plans from a risk register, which I think we're going to get to as well. So hopefully that gives a little bit more broader understanding of how we've broken out those risk themes and then who the different audiences are. The audience for that tactical is typically your your frontline who's working the the issues. Um, then the risk statements would be kind of that if you think hierarchical, you know, from a hierarchy perspective, um, you those risk themes and statements, the statements, excuse me will typically roll up maybe to like a VP, but then it's board level from the tier one statements.

Chris Logan: Well, you set it up beautifully because one of the things I love, this concept of those themes driving down to risk statements to tactical operations, is the work we got to get done. The problem is, is the work's never-ending, right? So, you know, and I'm going to jump to this next slide because you teed it up perfectly. Is that what do we do now with that work. Um, I know we have to track it. I know we have to manage it. How do we get rid of it? Who do we assign it to? How do you handle this right? If you think about the comprehensive nature of the theme to the statements, to the operational risk, what are you doing to help satisfy that need, to ensure that that operational layer is one being addressed and one being monitored at the same time? Because I think that's incredibly important as well. As you roll that back up into those statements and those themes.

Matt Christensen: I think it's important to to have an organization look at how are risks being identified and and by which means, and then, when they're identified,

Matt Christensen (cont'd): how they are being prioritized. And is it art or is it science, or a little bit of both? Yeah. So if you think about all the potential avenues that risk can come in, it could be through an internal audit. It could be by doing your annual risk assessment. Um, it could be an external auditor that was hired to, you know, pinpoint some areas of maturity. It could be a concern reported by an employee. I mean, there's a million avenues that these risks can then come in and then it's that okay. Now we know about this potential risk. How do we then understand? Is this something material? Is it something that we should, you know, put active resources on it right now? Um, you know, I think about log for J. Uh, that was, uh, what was that, December of 21 or something like that? It was that was a big deal when that came out. Right. And so while our team was still working normally, you know, our, our register and working our risk down and trying to just keep up. We shifted and put all boots on the ground to mitigate those risks and manage those risks within, you know, the log4j2 vulnerability. So I think the key would just be there's got to be a simple way for organizations to ingest all the risks, a process that can then vet and materialize.

Matt Christensen: You almost have to triage it. And forgive me if I use too many healthcare analogies, but that's the industry I'm most passionate about. You triage those those risks to then understand how big of a deal this is. How widespread is it? And then from there, you know, you can assign out resources. The thing I want to focus on is that not every risk that lands in the register ends up being worth it. Yeah. And that's that's a wild thing for some folks that have been in cyber long enough. That might just be mind-blowing, but if you know about it, you have to do something about it. And I don't believe that to be true. I believe that you can manage risk. And part of managing risk sometimes is just accepting risk for what it is. Um, you know, and again, we don't do that for the business. But if it's a big enough risk, you know, we can bring this forward and empower the business leader to say, yeah, we know about this, but we have these other controls in place. That means we don't have to stop Project A to fix this. What are your thoughts? Right. And then we have that dialogue with the business.

Chris Logan: That is wonderful. And this brings me back to a conversation I was having, I think, literally like last week. This wasn't a conversation we were having. I was having this with somebody else. And somebody had asked me a question about, well, how do I eliminate risk in my environment completely? I was like, well, you just stopped doing business. Yeah. Yeah. You shut the doors because it's not possible. It's not possible.

Chris Logan (cont'd): So I think what you said is spot on, and organizations really need to get their arms around that concept and ideas that there's some risk that's going to be acceptable. Right? Monitoring. Tracking and understanding that risk is what's crucial. That element is crucial there to understanding the risk and making sure that it doesn't grow from what it is. As the environment changes, as you bring new things into the fold, does that risk that you were willing to accept previously, which you're managing in your risk register? Has it changed so that it needs to be addressed? Now there's something else that needs to be tied into it to help lower the risk appetite or lower that risk threshold and create more of an appetite. That's right in there. Yeah, that's.

Matt Christensen: It is funny, too, when you come to risk acceptance. Um, I don't know if I should admit this, but I will. There was a time when I firmly believed you needed, like, a wet signature from someone to say, I acknowledge, I accept this, and I did this once. Actually, I actually asked for a signature because it was something that, from my perspective, didn't it? It didn't meet Matt's muster. Right? Like. And not that I'm always right, but it was an area that I'm like, we are taking on so much, right? This is in a prior organization. And the individual that had ultimate accountability said, I'm not signing that. I'm like, well, then you acknowledge that there's more risk than you're willing to take on. So please sign this paper. Right. He's like, I'm not signing it. You know, and I think that's the that's the wrong way to approach it. I actually believe the best way, when it comes down to something that material where you're like, cyber says, no, there's red light. You know, the wapper light is going full speed. Um, and we say no, and we need someone on the business to say, you know, I'm on the hook if something goes bad because of that. In my opinion, the best way to get acceptance is to then have that business leader collaborate with peers and the group. Think that out, right? So you don't hold an individual accountable, but you have a peer collective that says no, we all agree. Like if we accept that risk for what it is, you know, that lets us keep the other projects on schedule and we can provide better patient care. And then you start going back up to those risk themes, right? Yeah. That when you can get the conversation going back to the risk themes, I think that's a that's an indicator that your program is effective and that people are managing risk and not just mitigating risk.

Chris Logan: You said something here, and it made my ears go up a little bit because the next slide is really understanding. How do you start to justify your program or improvements? Can you drive that through peer recognition?

Chris Logan (cont'd): Are there opportunities for us as healthcare organizations to really focus on the benefits of what peer means and what we're hearing across the market and solve some of these risk problems?

Matt Christensen: Yeah. And so now we're shifting to peer among, you know, practitioners. Not necessarily, um, business peers. Right. So this slide really it's it's all about acknowledging that there's only one threat to cyber. And that's the adversary, you know, like. So when you can leverage data that can help, you know, in my investing two little in a program um or am I over investing, which is a risk that, you know, every good CISO has to acknowledge and say, are we bigger than we should be? Um, when you can look at how are other organizations that are of similar size? Where are they at? Is everyone scoring 100% and you're scoring 80? You know, because no one should no one should ever be at 100% on a benchmark. Um, but it does allow you to start looking at your program more holistically and saying things like, okay, we're showing, you know, we're showing more, more areas of risk within identity. And as you look across the board, other peers are doing the same thing too. That can be reaffirming, um, or it can be alarming, you know, depending on the benchmark that you're looking at. But as far as budget allocation, resources, all of the benchmarks themselves, you know, we use the benchmark within the sensor. Net platform. Um, tremendously. It's really easy for us to pull that out. In fact, looking at a prior board deck that was shown, you know, from our CISO, Eric Deckert, he's pulling these metrics right out of, you know, the sensor. Net platform. And then demonstrating to the board that we're not over or under-investing and that our our risk tolerance levels seem to be on par with the rest of the industry. And here are some areas that we may be performing above industry. And here are other areas that you know we need to work on and put more action place action plans in place.

Chris Logan: Yeah, and I like this concept and idea because I think it helps us build a narrative towards not just solving the operational risk issues that we're managing and monitoring but getting up to that mission and those key risk themes now because we have to communicate this up, right? And nine times out of ten, somebody's always going to ask, well, hey, how do we compare about these guys down the street? Um, but I think speaking in that language and allowing the board to truly understand that risk to where this data came from becomes incredibly important.

Chris Logan (cont'd): And it really leads into this next concept or idea is that now you've gotten that theme, you understand what that mission, what those statements are and the operational responsibilities are, how do you communicate it up and speak in a language that those business leaders, which honestly, probably a handful of your board members don't have healthcare experience, right? They're probably business people from outside the industry. How do you communicate those key themes to those individuals so they understand what risk tolerance is?

Matt Christensen: Yeah, I mean, it's like anything you have to know your audience. And in the case of a board of directors or senior executives, that's the audience that ultimately, you know, we're serving from a, you know, perspective, right? I mean, our ultimate audience would be our patients, our members, and the communities that we serve. But the ones that will hold us accountable is that is that senior, That is the senior audience. And so for me, it's understanding who they are, what their backgrounds are. I see a trend, Chris, maybe you've seen this too, that now, you know, cyber insurers, and it's more than just survey data, but it's actual, I think it's data that impact our industry. They're saying, how many of your board members have cyber experience?

Chris Logan: Correct.

Matt Christensen: And if the answer to that is 0%, which I would say across the board across industries is probably pretty true. You know, there might be some that have dipped their hand in it at one point, you know, dip their toe in at one point or another or have filled an earlier role or maybe were involved, you know, maybe they were a CIO and they were involved in some kind of like, vcdr type activities, business recovery activities, maybe. But most tend not to have that experience. And so if you can just know that right out, right out of the gate, then that helps simplify your your message to them. You don't report on those tier three very specific risks you focus on. Here's how we can impact patient safety. Or here, you know, here are the things we're doing to improve the likelihood of patient safety not being impacted by a cyber event. You know, um, I'm I'm not practicing what I'm preaching here because I've used a little bit of a monologue here. Uh, but I'm also passionate about it. You know, you have to keep your presentation data so clean, and you almost say, and this sounds bad, but it's like you make it to where it's junior high level, and you're not doing that because of competence. The more confused you make your audience, the less they're going to accept your message.

Matt Christensen: That's just I mean, that's one on one, you know? And so I think under putting it into their perspective, into their language is key, I think. Um, one of the best ways to help get support for the program, um, is, is making sure you're using metrics that mean something. Um, you can back those metrics up. Another way is by actually running exercises and saying, you know, we think we know how we're going to respond a, in a ransomware event. So let's test it. And then when you run those tests, I think eyes are opened. Um, and then you go back, and you report to the board, and you don't just hide. You don't shove everything under the rug that isn't pretty. Like, I think some of the best board presentations that I've seen do have more red on them than green. And it's not to send this alarming message, but it's being transparent about. Here are some areas where, you know, we're concerned about. It's having that needed conversation with the board. So, and then just to tie back to what we've been talking about, simplify, simplify, simplify. Get everything back to core themes, and you should define those for your organization and for your industry. Um, you know, make them easy and relatable.

Chris Logan: No. That's wonderful. Um, it's interesting because I agree with you. I think red's good. Sometimes, it's not for fear, uncertainty, and doubt. It's doubt. It's validation of assumptions at the end of the day. And that's what we're here to do. Help them validate those assumptions. Those tabletop exercises are a great validation point because the moment something's not available, the whole world stops. And I have a lot of examples about that, but I won't go into those examples. But I want to echo something that you said. I used to work for a larger organization, and the CEO there always had a common theme that he said, regardless of the situation, make your example Sesame Street simple. There is a there's a key message behind it, but it's understood by everybody. And I think we do that. We bog down in complexity. We try to make something so fancy to communicate upwards to that leadership when all we need to do is speak. Just speak the language they understand and frame it appropriately. So there's no question when you leave the room what you what you were saying right at the end of the day.

Matt Christensen: So Chris, along that line of Sesame Street, simple, which which I like now, now I have to naturally create a meme for that. But what I, you know, one thing that that I've heard over and over from our CISO, Eric Decker is this idea of is it possible or is it probable? And it's funny. The more sophisticated, the more educated, the more intellectual your leaders are, the more they simplify what it is they're teaching us. And we've known this.

Matt Christensen (cont'd): This is just humanity and in general, right? I mean, the deeper messages generally come with fewer words. And I think as we consider our board, one of the best ways we could give them good information is to say this is probable or this risk is possible, but likely not probable. Yeah. You know, and if we can help be that parameter and enable them, then they can start having those deeper conversations and saying, is this? Look, look, you know, they're saying that this is probable. Let's pause. You know, let's let's discuss this. Let's make a decision and then let's move forward. Um, and so we oftentimes need to be that barometer. But the more simplified we can make that message the more effective everyone is.

Chris Logan: Yeah. Fantastic. So we have a lot of people on the line. I want to make sure that we leave time for questions and answers. So we're going to lie down right. I have one more slide. One more bit of information I want you to share with our listeners out here. And it's about, you know, the cyber team's role when it comes to risk assessment. And what is your key takeaway here? What are you? Building in your group and your organization when it comes time to understand and assess risk. I do not approve of it.

Matt Christensen: There's this great image of a mouse approaching cheese on a mouse trap. And the mouse is walking up. You can Google it. You can find it. But the mouse is walking up and it's. At the mouse trap and it's got the cheese on it. And the trap is set and the mouse has the helmet on. And when I think of how we can manage risk, I go back to that, you know, that silly image. That mouse approaching the cheese again, a lot of cyber practitioners will say, can't do the cheese. Not worth it. Someone might die. We can't do it. Just can't. Right. But there's that compensating control of the helmet. Yeah. And that is we're managing that risk. And if it snaps, it's going to hit the helmet. I can get cheese in and out. Um, or transferring risk. Maybe we send someone in else to get the cheese, maybe part of it. But overall, our job is not to approve risk. It's our job to assess it effectively and present it in a way that executives can understand materiality. And then when asked and maybe if needed, we can prod a little bit, you know, here's our opinion. Here's what we would do. You know, when I'm treated as a patient, oftentimes I would say, well if this was your child, what would you do? You know, or if this was you, what treatment would you seek? And so, um, I think just getting that consensus I think is a really good way. So, yeah, I think that the overall message is that when we do assessments specifically like third-party assessments, we go in, um, depending on the level of risk of the assessment, we might go lighter.

Matt Christensen: You know, I'm not a fan of handing someone 300 questions. If all it is, is they're going to come in and put lockers in our, you know, in our gym, you know, no, no padlock, no network connectivity. All they want to do is just do that. Great. I don't have to hand them 300 questions to then feel good about saying that the vendor has had a completed risk assessment. Um, but again, at the end of that assessment, we like to use the term complete the assessment as opposed to what we've approved the assessment. Because the minute you use language and terminology and nomenclature like approval that you just rip, you just rip leadership, you know, from the accountable parties' hands. And now they're just assuming, okay, well, cyber said I can do it. So I guess I can do that when that's not the case. Our job is not to approve it. It's to assess and then to, you know, deliver those results. So it's one thing I love about the sunset platform is you have the option to say we've completed the assessment. And then when you hand that report, you say, here's the report that we've completed, you know, and here are all of our findings. These are the things that we feel you should know about that may impact tier-one initiatives and patient safety growth complexity confidentiality those ones. And by the way, here are some action plans that can, you know, you can do within timelines that can then manage that risk appropriately and then move forward. So just handing them that assessment is not your approval of it, but it's your completion of the assessment.

Chris Logan: Well, I love it because language matters. And I think that's every aspect of everything that we've talked about today language does matter across all of those steps. That's right. And if I think about, you know, what we've gone through and I'm just going to recap real fast. We started to talk about GRC, why it's so important to an organization, the language of the program, and how it's disseminated matters. It truly does to find that risk appetite and really look around. How do we align risk themes to be able to report up and simplify how we report those through a risk register, benchmarking against peers to create that narrative, helping drive the theme, and then communicating that with the board of directors? Right. Making it clear and simple in a language that they understand, but more importantly, understanding and assessing risk and not approving risk. At the end of the day, that's the real job of our assessors that we're tasking to help our organizations really start to define enterprise risk and start to deal with enterprise risk across all those different silos. So again, I'm going to stop talking. Is there any key takeaways you want to drive home in this last minute or two before we open the floodgate for questions?

Matt Christensen: I appreciate the opportunity to monologue even further. Chris. Um, look, I, I feel like GRC is far more than just a paperweight. We don't just have this, you know, ongoing widgets that we're cranking out. And we know about a risk. We do an assessment, we move on. I think our role is is to compile all of that risk that then comes in to use that professional judgment or in many cases, um, you know, a collective group think, but something that can get us more to science than, than, than art. And then being able to then roll, roll up the most important things in which we might need financial support for, we might need, you know, maybe we need to bring on contractors for a couple of months to knock out, you know, a material risk or to bring an organization back into compliance, whatever the case may be. But GRC is a function that I think keeps the rest of the cybersecurity engine going. And we can be used and I say used, but we can be leveraged, perhaps better stated in a way to help get more resources for a team. You know, if I hear this all the time, well, I don't have enough resources. Otherwise, I would do that because I agree with you, Matt.

Matt Christensen: That's something important that we should do. We should have enough resources and will leverage GRC to help write a report that can expose the risks. And maybe in doing so, you determine, like, yeah, that there's really not a material a lot of materiality in that risk. So it's not something that, you know, you're going to go stick your neck out on. But perhaps by doing a risk assessment, even internally, you can you can expose. Here are the top five things that, if we don't do that, you know, here are the associated consequences from it. Yeah. So um, that's probably what I would leave with is if anyone's considering GRC as a, as a, you know, a career or maybe you don't have a full team in GRC, just naturally, organically falls into an area of responsibility. Just if I could hone on one thing, it's we don't we don't own any. What we owe to the business is effective management of risk. And that's not always mitigating. It's not because mitigation is expensive. It's costly. It adds friction. It's just thinking things through and saying this is something that I feel like our organization is within our tolerance level. We should accept and I should I should make that recommendation to the business. And then from there obviously pass that off.

Chris Logan: Well, great stuff, man. Matt, I can't thank you more than sharing your insights, vision, and what you've done. I appreciate you joining me today and now. So, let's open the floodgates, as they say. Let's see what questions Matt can answer because he's the talent here. I'm just, uh, I'm just the moderator.

Matt Christensen: I know.

Saul Marquez: Well, fantastic job, guys. Uh, a really great discussion. Um, and so we do have a couple of questions, so let's, uh, tee those up. Um, oh, and by the way, your question, Matt. We got some responses in the Q&A. We got Boston and Hawaii, Virginia and Atlanta and Idaho. We got we got folks from all over the country attending today's webinar. So great to see the representation. And I love that question. Thanks for asking that. Um, any any tips for how to get involved with the GRC strategy at your org when you're not yet on the strategic job level?

Matt Christensen: Mhm. Okay. So I think that is my first response and Chris, I'd love to hear your thoughts too. You don't need to have a title to have influence at a strategic level. And I believe that firmly. It's a certain title might get you into a meeting or into a discussion, but that isn't what equates to influence. Some of the best risks have been identified by people in our organization and prior organizations. I've worked at that that don't have these, you know, big titles. Right. But they see something, they say something. Um, and they put it in a way where it's like, oh, wow, this could directly impact patient care. Um, so we often will refer to, you know, just if you and I, it's a government thing. Right? But see something, say something. Um, that's probably the best way. And then I think just in getting involved and getting educated on what risk tolerance and appetite even means, what's the difference? Um, what would you anticipate your organization to be like? What are the speed limits for your organization and for your industry? Um, and then the third thing I would say is just get educated in this space. There's no shortage of GRC podcasts. There's no shortage of opportunity to get involved with, you know, some of the like ISC square, the isacs of the world. But, um, start participating in those local chapters because that's where you'll typically end up meeting people like Chris, uh, who you can then bounce things off of. Um, but yeah, that would be what I would say. What would you add, Chris?

Chris Logan: Yeah, this is this is a very interesting question. I like this question a lot because it really starts to get at the heart of culture. And I think culture is probably the most important element of any organization. It's not all a fancy tool we have. It's about the people. And if I start to think about the culture that we want to build in our organizations, you want a culture of transparency and you want a culture of courage. And what do I mean when I say a culture of courage? Everybody has a voice. And again, you see something, say something. I know it's a government thing, but there's a reality here, especially in the field, that we work in.

Chris Logan (cont'd): If you're in a healthcare provider organization, it's really your responsibility that if something does not look or feel right, you have to be able to speak up and say something. So as a leader, I want to encourage that in my staff. And even if that staff member is not a part of the GRC program, I hate to say you've said this to me before and I'm going to reuse this again. Everybody in your healthcare delivery organization is a caregiver, first and foremost. I don't care if you work in the laundry. I don't care if you work in the supply chain or in it. You are a caregiver because there's something that you do on a day-to-day basis that's going to impact patient care along the way.

Chris Logan: So having that transparency and the courage to stand up and say something, even if you have to take it up the chain, do it in a very humble manner, but do it in a manner that creates a sense of urgency around it. When you see that that's what we want to build, that's what any good leader is really going to start to drive and push for. Now, getting involved in the GRC space, that's easy. You don't have to be a GRC analyst to be involved in the GRC space because GRC is not pervasive across the organization, but it's present across the organization, as Matt has alluded to. Right? It's not a single silo effort or energy. You play a role somewhere along the line of understanding governance, risk, and compliance in your organization. You have the ability to add that influence as well. And we should be really thinking about training our people across those boundaries, because a workforce that's more diverse in thought, more diverse in action is going to be what, just a better workforce and uncovering areas that we need to start to address, right? So, really, that transparency, that courage, and getting people involved at all levels is critically important to our success. And what we're trying to accomplish is a better outcome for the patient at the end of the day.

Saul Marquez: Thank you, Matt. Thank you, Chris. And if there are any follow-ups to that, please go ahead and put them in the Q&A. We also have Ohio in the House, so I want to call them out. I've got a plug for Ohio there. Um, this one is a little off-topic, but is Cincinnati doing a benchmarking study this year? I heard a fall at one point.

Chris Logan: I guess I'll take this one because Matt probably doesn't have the answer. Yes, I.

Matt Christensen: Have a suspicion.

Chris Logan: A sneaking suspicion, yes, we absolutely are. We'll be kicking this thing off really shortly. We're looking for more participants. We're going a little bit deeper into the well to make sure that we're addressing those areas from the previous benchmark survey and expanding it to give you more rounded, more robust information. Simplest way to get involved? Send a quick email benchmarking@cincinnati.com. You send an email to that. It'll come to a whole bunch of us over here. And we can start that process with you to get engaged and be a part of that next wave for for benchmarking.

Saul Marquez: Thank you, Chris. And we're getting a lot of thank yous here. So just want to give you Matt and Chris kudos for a great webinar today. And thank you all for for the questions. One that came up is repeat the email address for the CEUs. Just as a reminder, everyone, you'll get an email After this webinar, you'll receive a recording of today's webinar. The slides reply to that email, let them know that you want those credits, and they'll respond uh, very quickly to make sure you receive those. So we are here at the end. Uh, we're no more questions in the Q&A. Is there anything else, uh, Matt and Chris, that that you wanted to to, to close out with?

Matt Christensen: Yeah. I'll conclude. And then Chris can kind of sweep the floor as it is. Um, just the huge thanks to, you know, for putting this together. Uh, thanks to Sensor Net for driving the questions and the content. Um, I, I love working in cyber, and I love working in healthcare. You don't have to go too deep in our family to understand why I chose healthcare. Um, and I won't get into those details then, but I know my why, and it's rooted around helping people live the healthiest lives possible, which is, you know, Intermountain Health's mission statement. And when I can do that in a way where cyber can directly impact people living their healthiest lives, there's meaning to that. So it gets you through, you know, the 14 hour of back to back meeting that occasionally will happen. You guys say risk never sleeps. I often think I never sleep. Um, you know, but knowing your why can really, I think, drive a wonderful career in cyber. Um, and the last thing I would just throw out there for the attendees. Can I love to connect on LinkedIn? I'd love to hear your story. I'd love to know if you've been in cyber or if you're thinking about, you know, changing careers, if you think about GRC. So please find me on LinkedIn. I'm I'm somewhat active on that platform, but I'm always responsive there. So thanks for the opportunity.

Chris Logan: Yeah. And I just real fast I want to echo that and thank Matt for his participation. And really thank all of you for joining us. I mean, this has been a journey. We came up with this idea and we started this because we wanted the voice of the practitioner to be heard. We wanted the practitioner to understand how they could get out there in the enterprise a little bit deeper, how they could better their career and train a little bit differently, and then how we can escalate what we're doing on a day-to-day basis. This isn't the end for us, right? There's going to be something else. We're going to do this same type of form and fashion. But really, again, thank you for participating in this series. And more importantly, remember this is a team sport. I can't stress this enough. There's no one single person in healthcare delivery that solves any one problem. It's really a team that's going to solve that problem, whether it's on the care side, the administration side, whether it's even in research and development. There is a team of folks who are focused on improving that outcome for that patient.

Chris Logan: And we, in the IT side of the House and the risk side of the house, are a part of that. We are part of that linchpin that's holding this all together to help people understand their role. What their responsibility is and how we can assist them to drive that better patient outcome. So again, know your why. Why am I here? I love the mission of healthcare. I want to leave it just a little bit better tomorrow for my kids to take advantage of than what I'm dealing with today, right? So if I can do that in some form or fashion, by God, that's what I'm going to do. But it's going to require all of you on this webinar as well. I can't do it myself. I need your help and I need your support. So I greatly appreciate your time and attendance and your attention. Do you need anything at all? You know where to find me. I'm pretty active out on LinkedIn, Matt, so they can find me pretty easily and I will direct them to you. Don't you worry about that?

Matt Christensen: Not worry about that.

Chris Logan: Again, I appreciate everybody's support in this journey. Thank you so much for your time and attention. Have a wonderful day.

Saul Marquez: Yeah, thanks, everyone. Have a great day.

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