Podcast Transcript

Risk Never Sleeps
Episode 78
Steven Ramirez

Ed Gaudet: Welcome to the Risk Never Sleeps Podcast, in which we learn about the people who are on the front lines, delivering and protecting patient care. I'm Ed Gaudet, the host of our program, and today, I am pleased to be joined again by Steven Ramirez, the Chief Information Security and Technology Officer at Renown Health, Steven.

Steven Ramirez: Glad to be here.

Ed Gaudet: How are you? Welcome.

Steven Ramirez: Great. Thank you.

Ed Gaudet: Yeah. Welcome back. By popular demand, we had a lot of folks who were interested in your last episode.

Steven Ramirez: That's the way to be. Yeah, yeah. Glad people watched.

Ed Gaudet: Yeah, we talked in October. So I'm sure a lot's changed since then, and no pun intended. What's new with you?

Steven Ramirez: A lot has especially changed in healthcare. I know that was the biggest thing a lot of CISOs across the industry were looking at. So I know we talked about third-party risk and access, and that was really those themes played over to what happened with change healthcare. So I think that brought to light a lot of healthcare organizations have been focused on patient care operations, and I don't know that we would have ever thought something like an exchange or anything like that would be. And the vast impact that would actually provide for downstream, it would do for a lot of organizations. And then, having a lot of eggs in one basket, we realized that for some of these critical services we need to start having backups for backups. Yeah. And really, going through our holistic process, we were just scratching the surface of third-party risk. Now, it's really important that we didn't even really have a third-party risk assessment because we were going back and switching tools and going back to really look at that, and we're going back holistically doing a lot of our lessons learned. We're like, really? How do we measure up our business continuity side, our most critical vendors, and our critical applications and services from that vendor? With some of our high-risk vendors having a dashboard to be able to maybe have that foresight and crystal ball into some of these components might have changed some of our response and our overall business continuity planning. But I think that change in healthcare just definitely brought to light the necessity for a strong third-party risk program, not only just doing the assessments, but also the mitigations and then the downstream supply chain risk. So that's getting into how that can impact your business and making sure they're not a single point of failure. So, can you have multiple service offerings to that? Backups. As you know, we pivoted from some of the tools that they were using on the pharmacy side over to the McKesson side because they have an Rx offering, just because of the sheer vast impact of all of that. I know a lot of other health systems were more impacted than us. Specifically, we had a health plan, so that was probably our most impacted, as well as our pharmacy processing.

Ed Gaudet: And how quickly were you able to start recovering from the event?

Steven Ramirez: I think there's a good lesson also on Hicks and putting together your incident response and bringing these players together and shining into light the importance of third-party risk and contingency planning because you're just basically living and breathing it day-to-day on, like, okay, this isn't working, what's our workaround or what our vendor partners can we look at?

Steven Ramirez (cont'd): We had a lot of workarounds we were able to do. I know we were a long-time customer of change, especially on the health plan side. So that gave us a little bit. Yeah, more flexibility to start to do some of their rebuild systems getting on that list earlier on, but we were just looking at other vendor partners' workarounds' manual, a good old-fashioned way of calling pharmacies' paper scripts and calling and doing the old-fashioned insurance verification. So again, that's the importance of downtime procedures. So I think we're able to test a lot of that. But again we were impacted but not as impacted as others. But it was a good lesson learned and exercise to go through that for this event. But prepare for other events.

Ed Gaudet: And to your point about business continuity and being able to recover, not just bring the program up, but also have alternatives that you can draw from right out of the gate, I think that is a real lesson that we can take from this event as an industry.

Steven Ramirez: Definitely, so we're looking at backups to some of these critical services and actually doing an exercise to start to holistically look at our top vendors, our critical vendors by service line, and then tying that into our riskiest vendors. So if we have somebody that says your top five and say, our surgery pharmacy line, our pharmacy, our surgery service line, and that based off of those five they give us, do we have all the risk assessments for them on file, and where do they really rank on that? Because we're starting to look at putting together profiles by workstream like that to then say surgery as this kind of school, pharmacy has this kind of score, and med surge, really looking at how we can help the business make more strategic discussions when we're looking at advancing things in our strategic plan. So that's something that we're really scratching the surface. And I'm spending a lot of time with our Chief Analytic Officer. He and I actually went to HIMSS together to look at some of our technologies together. And he's helping me create tons of dashboards because, you know, the best way to make decisions is having the data. So he's been a great partner and taking data from here, data from there, and combining it together. So he and I have been in lock and step on really putting together a lot of this to have more risk, data-driven risk, and insight decisions throughout the organization and bringing that to our governance risk, Biden's committee, our audit committees, etc.

Ed Gaudet: So you went to HIMSS. How was it?

Steven Ramirez: Great. It was the most packed. I've seen it since pre-COVID.

Ed Gaudet: Wow. Awesome.

Steven Ramirez: Yeah, the floor was pretty exciting. There were a lot of great events. It was great to see a lot of vendor partners and fellow providers in person. So I went to the cybersecurity forum but also went to the CXO. So to go in there and see what's going on in the innovation side. So, I think that really the biggest takeaway was AI automation. We're looking at 5G. So really is a, you know, being the tip of the spear on different network connectivity within the hospital. So working with some partners on that. But yeah, it was definitely AI; took everywhere we went. That was really the key topic and takeaway from everything.

Ed Gaudet: No, I love that, I love that. And did you go to ViVe or just HIMSS?

Steven Ramirez: Just HIMSS.

Ed Gaudet: Just HIMSS. Okay.

Steven Ramirez: Last year, at the end of last year, the HHS announced new cybersecurity performance goals. How were you thinking about those over the next 12 months? I think it's great that they've done that. It's very similar to what the 4 or 5D and HICCUP have done to really make things more palatable and bite-sized key areas to look at. What we did was look at what the goal and the essential goals are, looking at where we aligned, and then doing a crosswalk to our CSF. And then really, you know, painting the picture of those risks mitigated. And I know they break that out into two different pieces: the essential goals and then the enhanced goals. So that's really going into our roadmap to make sure that we're really covering all these various baselines, not recreating the wheel. I know there's a crossover from the CSF, but making sure from the hiccup and these new performance goals that we're really making sure we're covering everything because they might become mandatory at some point, I would envision. So making sure that we stay ahead of the curve and just put that into our overall program documentation.

Ed Gaudet: Yeah, no high probability they will become mandatory. That'll be true, given your first look. How are you doing in terms of coverage?

Steven Ramirez: So, from the essential goals, it's looking like we'll attain all of them. It's just about our maturity to all of those similar to NIST. So it's I'm just continuing to build that maturity. You know, we're hitting threes usually in that very high twos, maybe in some of them too. And that helps us really put together our roadmap. Maybe I'm looking at things that we weren't looking at from a different lens, from just the vast pieces that NIST puts together. So that's something also when we're doing our roadshow with the business to really help show the importance of what we're doing with our technologies when we're vetting our third-party partners, etc., on that, to really show them that. I think this is a good way to show some of those key fundamentals in security.

Ed Gaudet: I love that, and as you look at new technologies such as AI, how do you think about bringing AI into your organization and what have you done to date to help with risk mitigation or at least risk identification?

Steven Ramirez: So when the buzz of AI came out middle of last year, we came together as part of our governance, Risk, and Compliance or GRC committee to really look at how we wanted to tackle that holistically, starting with ChatGPT and all that. We're pulling telemetry on how much it was being used, and we thought that we would maybe take more of a back seat. Not that we don't want to be innovative and utilize it, but we're not going to be creating our own AI technology in-house. So we're taking the stance that we're more going to go with when Epic releases AI-based modules or Microsoft releases Copilot like they have that we're going to start really crawl before we walk with some of these embedded and baked-in tools from some of these trusted partners, versus us trying to think we're going to be bleeding edge and create our own technology, because that's where it will really get into, you know, higher risk scenarios. If we're trying to do stuff on our own, how we're protecting data, and looking at all these different fundamentals that we need to put into place. So we're really taking that kind of more liberal approach or conservative approach, I would say, to just making sure that we're utilizing these tools as they come out in some of our more trusted partners with, again, Microsoft, Epic and other pieces like that, and it's going to just come out more and more same on the security side.

Steven Ramirez (cont'd): There's some machine learning that has been done for a long time, but we're treating the intake of that no different than any other new vendor or technology that if we see something as part of our process that is AI-based, that goes to me or chief analytic officer and our IT applications. So the three of us look at it to see if it's something that we could either parlay into something that another vendor has. If this is something that we're willing to take on and can put into our kind of strategic roadmap or something that we would even want to build, maybe down the road we have the go-no-go as part of that, but to go through and do our various security assessments. If it's a net new assessment to that, to look at what it's really collecting, how it's being protected, seeing if our agreements are all up to date on that.

Ed Gaudet: Now, is that all the way? Does that include clinical applications, or do you have another group that looks at clinicals?

Steven Ramirez: We look at all of them coming. Yes. So our chief analytic officer is very versed in a lot of that. So I know he's got a lot of good components and background in that. Especially as he's building that enterprise data warehouse. So we're doing a lot of in-house development. So he's trying to see if this is something he can create at that subset because AI is only as good as the data it's getting. So if that's something that's on his roadmap and everything that he's looking at, and we already know we have our data warehouse secured. So we're not going to try to create risks that we're not prepared for just to chase the shiny, bright object.

Ed Gaudet: Yeah. One of the challenges we found is setting the right policy balance with the adoption of emerging technologies like AI, with the protections that obviously get us into trouble if we go too fast. How are you thinking about that from your user community, especially where AI is such a great tool to increase productivity in many different dimensions of our day jobs, right?

Steven Ramirez: And that's what we're looking at it from a use case perspective. So, like copilot has so much potential on being able to help us with burnout. A number of meetings, meeting minutes, some of these low-hanging fruit stuff that isn't necessarily PII or PHI.

Steven Ramirez (cont'd): So if we're able to get that really good, we can start to morph that into how else we want to use it throughout our various clinical areas and administrative areas IT, data analytics, finance, HR, and some of our support services. We'll look at really piloting it with them because we don't have as much data as some of our clinical stakeholders, but also see what kind of technology would make sense for a nurse versus a supervisor versus for our providers versus med assistants. So it's really looking at almost role-based access on how they would use it. You know, are they just users of it, or are they able to go in and manipulate data? So that's also tying back to our data governance program. So that really shows the importance of that. And good old fashioned DLP data classification and data tagging and a lot of that that you can't things can get out of control pretty quickly if we're not keeping a good pulse on that and governing it.

Ed Gaudet: No, I love that. And are you thinking about those areas of AI, maybe to consider bringing in internally and building out your own infrastructure to deal with a lot of security and risk issues accordingly?

Steven Ramirez: Yeah. So I know that there's a lot of specific to security for insider threats and seeing just different anomalies. We're looking at that from one of the NDR tools that we brought in. A lot of the EDR agents have had that for a long time. So looking at different anomalous behavior, but really seeing how that can correlate into a sore. So, how can we automate isolation? Because again, if it looks like a duck and quacks like a duck, it's going to be a duck for some of these low-hanging fruit or risks that we know about. So we're trying to see how we can action that with our security partners, with various run books. If this X happens, it's got a 95% validity based on these other data sources. How can we automate that with various AI-based technologies on the security side? Because, again, if we're using AI for business operations, threat actors might be using that. We need to look at how we pivot to that. We've even had to pivot to a more AI-based tool for our email and phishing security just because of the onslaught of what we were getting. So that's where this emerging risk comes up. We had to go out and look at our problem statement as an organization that we have a way of manually forwarding. We have our SEG tools that look at this. So were they really meeting the threshold, again, using data to go through and drive out to procuring a new tool that integrates in? And we've seen a drop in almost 700 phishing emails a week and almost 6000 a month.

Steven Ramirez (cont'd): So that's where AI can, again, on the security side, go through and analyze these emails very quickly. We're seeing emails still the most effective threat vector out there. So again, that's something we're continuing to focus on. Still require our users or our frontline defense. So we're making sure that they go through. We give them good training and awareness but still have this tool. Like the lane assist in your car. You can only do so much energy. What we're doing to make sure that keep user error out, there's always going to be that human factor. So, how can we supplement and keep our users from getting more of those phishing emails in their mailboxes?

Ed Gaudet: How often do you do training? Are you doing it quarterly or monthly?

Steven Ramirez: We do our annual security and awareness training. We've been doing a lot of monthly phishing training now with some good education into that, but we're also putting pretty complex phishing use cases out there. Our last one was, you know, add me on LinkedIn. So I got a lot of people that reached out, and I'm explaining to them that you probably don't have your LinkedIn tied to your renowned email. You think that good educational standpoint. So that's brought to light on some of these various use cases. And again, that's where I'm working closely with my chief analytic officer to build out our phishing compliance and education program from this data. We have about 5 or 6 months of trending data. So, let's start to look at again work streams. So, our clinical users look like they're the biggest people clicking on things. So they need the received emails externally. Is there more targeted training? We need to have additional discussion. So that's partnering from the data side, but also with our compliance and HR to start to look at it from the human side. What do we need to do from targeted training? Something that I create might not be something that translates over to a nurse and what they need to see. So we're going to try to take that out to see how we can continue to develop better training. That better helps the end user to see what they need to look for, to provide them the tools to do reporting not only for phishing but for any anomalous activity.

Ed Gaudet: I love that. And last time we spoke, we talked about priorities. What are some of the adjustments you've made over the last six months or so to your priorities over the next 12 to 24 months?

Steven Ramirez: So third-party risks' are still up there. So just growing out in the tentacles of that, getting into the fourth party, looking at more of the continuity. So DCDRs are even bigger on making sure not only recovering a technology if it's in-house or impacted by a vendor but also the continuity side from having backups, having downtime procedures, testing, and doing that a lot. Also, access management continues to be vendor access management. I think we as an industry, if anything, change healthcare also showed information sharing, people doing various updates, and I think we're able to cut and sever connections and quarantine emails haul pretty quickly. Yeah, after us all, just having good discussions with peers on what's going on. So I think that's getting better on events like this, just how you can do some real-time information sharing with other health systems out there. Also just getting more into automation. So we're having a lot of these tools. People have had our EDRs or MDRs, our NDRs or EIEIOS forever. So how do we start to integrate these and get that real-time intelligence and quarantine? We've talked about that for a long time, but really starting to action these things, doing true segmentation. And that's where we see a lot of potential with 5G taking like a lot of our bolt and BYOD devices and other telephony-based devices. In the hospital, and just moving that off, but also being a redundancy if we ever have a network outage, really exploring that kind of cutting-edge technology to see how that can help segment stuff just by design. On maybe putting legacy-based devices on that, having different VLANs and other pieces that we've talked about for MOT IOT, and there's a lot of opportunity for that. So we're excited. And that was something that we looked closely at HIMSS as well for putting together a roadmap for that as well.

Ed Gaudet: Cool. That's great. So, I think last time I asked you a bunch of personal questions, so we won't rehash those, but anything that's new on the personal front that you'd love to share with listeners?

Steven Ramirez: I'll get married in October, so that's going to be that might be the riskiest thing I'm doing if I had to go back. So I was excited for that.

Ed Gaudet: It is the riskiest thing, by the way, you've ever done.

Steven Ramirez: So on top of that, the day-to-day stuff, it's the wedding planning and all of that.

Ed Gaudet: Nice. Congratulations.

Steven Ramirez: The bachelor party also might be one of the riskiest things.

Ed Gaudet: Hopefully, it won't be. Yeah, you're not 20-year-old anymore, you know. Stay out of Vegas.

Steven Ramirez: Yeah. Going somewhere warm with some sand, but yeah.

Ed Gaudet: There you go.

Steven Ramirez: Everything's been good. It's been really enjoyable to see where technology is going and really see the direction our organization's going. Our senior leaders are doing all of our strategic planning. So, really excited to see where our growth and key focus areas are because then that enables us from the security and technology side to help put together our tactical plan to support the business. So some are just exciting times in healthcare, Renown, and obviously leading up to the wedding.

Ed Gaudet: Yeah, and you're not a kid any longer. But the kids these days don't do their honeymoons right away. Are you going on a honeymoon right away?

Steven Ramirez: Right away but that's our biggest discussion on that. Security professionals are always on our phones.

Ed Gaudet: I know.

Steven Ramirez: Especially adding the CTO to the CISO side of the house. We're trying to see how long I can make it without getting a call or text for three days.

Ed Gaudet: Weekends and go like a Friday through Sunday.

Steven Ramirez: We're going, yeah, we're trying to do 7 to 10 days.

Ed Gaudet: Oh, nice.

Steven Ramirez: So we're excited about that. So, I told my team there was a PTO freeze. Nobody else is able to go on vacation, and we have everything tied up. And it works well because going back to change healthcare, I was out of the office on a golf trip when a lot of that happened. Not that I wasn't getting texts and keeping close with my team, but being in a country that really shows that was a good exercise to have some of my keys.

Ed Gaudet: Yeah.

Steven Ramirez: Security members to go in and get some good visibility and run with the exercise.

Ed Gaudet: Where you in Scotland, playing golf or Ireland?

Steven Ramirez: I was down in the Dominican Republic.

Ed Gaudet: Oh, Dominican. Oh okay. Okay. Yeah.

Steven Ramirez: So it would have. Yeah. It was a good chance for my team to have back which goes into contingency and other stuff that sometimes there's leaders that won't be able to be reachable. So it's we're going to use that mentality and hope that it's smooth sailing for 7 or 10 days with, knock on wood, no security issues or third-party issues.

Ed Gaudet: So now, are you sun and sand or are you thinking about going and doing a Europe or what do you tend to?

Steven Ramirez: Sun and sand? I think we're going to do Hawaii.

Ed Gaudet: Oh, that's awesome. That's terrific. I just got off of a two-week stay in Aruba. Have you been to Aruba?

Steven Ramirez: I have not, but that's. We're going to a wedding end of the year there as well.

Ed Gaudet: So it seems like whenever we're there, there's always our third year in a row, and there's always a wedding on the beach. We stay.

Steven Ramirez: Yeah, excited to that.

Ed Gaudet: That'll be nice. Yeah, yeah. Excellent. Any last comments or thoughts for listeners before we break?

Steven Ramirez: Great to talk to you, as always. And yeah, so maybe when we talk again in six months, we'll see. Yeah, yeah. See where things continue to progress.

Ed Gaudet: Maybe after the wedding, we can do a wedding follow-up. How about that?

Steven Ramirez: Yeah, definitely. Things will have changed in November.

Ed Gaudet: Yeah, yeah.

Steven Ramirez: We're just waiting to see what the next big thing is that changes healthcare. Anytime something happens, it would do us a disservice if we don't learn from those two.

Ed Gaudet: Oh, we learned a lot from this one. They just keep getting bigger and worse. And the tendrils that change had in organizations, and I think, what was it, 60% of the hospitals that were affected were losing $1 million a day or more. It's just incredible in terms of the impact it had in a short period.

Steven Ramirez: And a lot of people probably didn't think that the level of magnitude of losing something that or how critical it was, and did have a downstream impact and no insurance authorizations on the pharmacy side. It had more of a patient care impact than a lot of people would probably realize. So it's definitely an eye-opener as we continue our emergence to pushing more out to vendor partners, going to the cloud, the importance of good security hygiene, and then having a good third-party risk management program to weigh it. It's the same; that's not a question of when or if it's when. So have that same mentality for your third-party partners as well. So, having a plan B.

Ed Gaudet: Be prepared because the next one may hit you directly. That's a great way to end the program. Thanks as always, Steven.

Steven Ramirez: Pleasure. Great to talk to you.

Ed Gaudet: Checking in to talk to you. Yeah, it's always great to talk to you, and I look forward to catching up with you in November after the wedding and the honeymoon.

Steven Ramirez: Sounds great. Thanks again.

Ed Gaudet: Thank you. This is Ed Gaudet from the Risk Never Sleeps Podcast. If you're on the front lines protecting patient safety and delivering patient care, remember to stay vigilant because risk never sleeps.

CENSINET®

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 DEMO

www.Censinet.com