



Rockin' HIT Sales

Episode Transcript

Cybersecurity, Vendor Trust & Security Review: What Health IT Companies Need to Know

Guest: Gary S. Chan, System Vice President and Chief Information Security Officer, SSM Health; Security Mentalist

Release Date: September 23, 2026

Transcript note: Edited lightly for clarity and readability. Intro and outro omitted.

David Hacker (01:02)

Gary, welcome to Rockin' HIT Sales. I really appreciate you joining me today to help our listeners get a better understanding of healthcare cybersecurity, vendor trust, and what Health IT companies need to prepare for before they enter a provider environment.

Gary S Chan (01:21)

Hey, thanks for having me on your show. I'm happy to be here and love the topic.

David Hacker (01:27)

How would you describe your role as Chief Information Security Officer inside a large health system like SSM Health?

Gary S Chan (01:37)

Well, I think I should be called Chief Meeting Officer, because that seems to be the only thing I ever do. At a large company, as you move up the management chain, more and more of your day is spent in meetings. So essentially that is my day. I'm meeting with other management to understand what people are doing. I'm meeting with my management to tell them what I'm doing. I'm meeting with other people to influence them to agree to what I want to do. I'm meeting with people to tell them they shouldn't be doing something they're doing. I'm meeting with vendors who want to sell me stuff. So it's just meeting, meeting, meeting all day. And then at the end of the day I get around to my emails, which is really just setting up more meetings. But at least it's a change.

David Hacker (02:26)

I've often seen leaders' schedules, and I see them double- and triple-booked and ask them, when do you do your job?

Gary S Chan (02:34)

After hours.

David Hacker (02:36)

When Health IT vendors hear 'security review,' which is a normal part of the process, what do you think they most often misunderstand about what security review actually is?

Gary S Chan (02:47)

I think a lot of them don't know what it is, especially if they're a smaller company. If they're a bit larger, they usually think of it as a check-the-box type of review. And if they're really big, they tend to understand what it means. They understand that it is about the buyer doing a risk assessment and asking: Is this going to cost me anything beyond what I'm paying the vendor? Maybe I need better insurance, or maybe doing business with you could cost me some customers. There's a whole bunch of other things that happen when you do a security review. Those are kind of the three tiers I'd put them in.

David Hacker (03:27)

When companies think about cybersecurity, how should they think about it as part of trust, adoption, and safe scale, and not just as a technical requirement or, as you just identified, checking the box or filling out the spreadsheet?

Gary S Chan (03:44)

It really boils down to trust. I think the easiest way to understand that is to think about buying something yourself. Don't you consider the risk of it causing harm? Say you buy a toy: Is it going to harm my child? You take that into consideration. These IT vendors and their solutions are so much more complex than a toy car, so you have to understand a lot more in order to properly assess that risk. Is it going to harm my patient? Because if it harms my patient, that's probably a really bad thing. As a patient, would you want to go to a hospital where they say, 'We'll put you in our MRI machine, and 80% of the time people come out fine'? Or if they said, 'Ten percent of the time your data gets put under the wrong patient chart or ends up online'? Those are exaggerated examples, but they illustrate the point. What security teams are doing is not really different from what a normal parent or person does when buying something for themselves or their family.

David Hacker (04:56)

You just touched on that, and I'm going to dig a little deeper. How do patient care, operational continuity, regulatory issues, and organizational trust shape the way security teams evaluate risk?

Gary S Chan (05:10)

They each have pushes and pulls, because what we're always doing is trying to balance all of those things. If the vendor is selling something that is very, very beneficial for a patient, then we're going to want to do more and may be willing to invest more in the security portion in order to make it work. Maybe we'll make some sort of exception because the product can't do a particular thing and we need a certain level of security. But if there are a lot of competitors and other competitors have what we need, that could shift the equation toward buying from someone else.

How much the product benefits the patient is a huge factor. With regulations, I don't have a choice. Auditors come in every year and look at what we do, what we approve, and our processes. If they ask why I approved something that was very likely to cause harm or loss and I don't have a good answer, there can be a fine. So I might not be paying the vendor, but I'm going to have to pay the government. That's a cost that has to be considered.

Then there is operational continuity. If I buy your device and every patient has to go through a process that depends on your machine, and your machine fails, now I can't provide patient care because the process depends on your product. Of course we'll want fail-safes. The vendor may love it if I buy two of them instead of one so I have a backup. There are all sorts of things to take into consideration. When I do a security review, I may ask, 'Does your stuff fail?' The honest answer could be that it does and it fails a lot. The right answer may be that I pay you more because I'm going to ask you to develop high availability or give me two of them. Bad answers are not always bad for the salesperson. Each of these factors has a different push and pull.

David Hacker (07:38)

This is a question that comes across everybody's mind as they're going through the sales process: How early should vendors start addressing security expectations? The sales process may start in an operational department because they want to make sure they have a need that the solution will address. Those operational leaders might not have security top of mind. So how and when should vendors start bringing the security issue to the surface?

Gary S Chan (08:17)

I would say at two points in time. One is before you even go to sell it. This stuff is not a secret. All healthcare organizations are going to want the product to have good security, so you should be able to do that assessment on your own before you even try to sell. That's the first point.

To answer the spirit of the question about a specific organization, they usually start with the operational leaders first because, frankly, if the operational leader doesn't want to buy it, your having good security is irrelevant. But I would say security should come in basically right after that. That's the way it works at my employer. When the operational leader says, 'I'm interested. I like this,' that is when they engage us, or the security team, as part of the process to evaluate whether the security needs are there.

The biggest issue, especially for newer salespeople, is that they can be surprised by this step. They sold the operational leader on it. The operational leader says, 'Yes, I want to buy it,' and maybe says their boss agrees. The salesperson has already popped the champagne bottle and thinks they sold it. Then security comes afterward. I think that misunderstanding is where a lot of the frustration happens, because they think something new was added when it was actually just part of the process. That's something salespeople learn over time if they stay in the business.

David Hacker (10:01)

I often tell customers that getting operational approval is just step one of many steps, and it's going to be a long ride. So when vendors enter security review, what are you really trying to find out and understand about the solution and the organization?

Gary S Chan (10:21)

A couple of things. At a high level: Is the product or service you're providing actually secure? And I would also say intent matters. Your product might be secure, but if your culture is incredibly insecure because you really don't care and you're doing things strictly to sell it, that makes a difference. That comes out in the conversations. You get a sense of it.

You can ask some very basic questions, like: How many people are on your security team? If you get crickets, then even if you have a wonderful report that says how secure your product is, I'm probably not going to believe you. You're looking at the controls that are in place, but you're also looking at the culture. Is this a company that will care? If I find an issue, are you going to issue a patch?

Did you do an independent assessment, or did you just have an engineer with no cybersecurity experience tell you it looks good? Or did you put it into ChatGPT and ask it for the right answers? I've had people ask ChatGPT to give them the right answers, and it answers randomly because it doesn't even know the product. It's not an exam from school. That's really what we're trying to understand.

David Hacker (11:46)

Are there behaviors or things a vendor can exhibit that build confidence from your perspective in the solution and its security?

Gary S Chan (12:00)

Absolutely. The ones who are well prepared are obvious. If they say, 'Give me your security questionnaire,' I already know I'm probably going to get a good answer because they know that is part of the process. If they have any third-party endorsement, such as a certification, an ISO certification, a SOC 2 report, or even an outside IT consultant who signed off on it, that's a very good sign. An external party that signed off or performed a penetration test is a positive signal.

And if they have an actual person on the team whose job is solely information security - not just part of their job, but 100% of their job - that's another very good sign. You can ask whether that person is focused on the company's internal security or on the product being sold to me. If they say they have one for the product and another for internal operations, those are incredibly good signs. Assuming they're not lying, those things get weighted very heavily, much more than whether they can answer a question about 256-bit encryption. Everybody is going to write 'yes' to that at this point, and you don't always know whether it's true because you can tell from the questionnaire what the expected answer is.

David Hacker (13:37)

You mentioned outside certification. Besides certification, is there other documentation or preparation a vendor can provide that makes the security team's job easier when evaluating the solution?

Gary S Chan (13:53)

Yes. Any document that explains the architecture and, at a high level, the policies and practices they have in place helps. They don't have to give me every policy; they can tell me they have policies and explain the different things they do. If they use a specific framework like NIST CSF, tell me that. It's really about giving someone confidence that you've invested in this. Any kind of preparation gives the buyer more confidence.

David Hacker (14:32)

You're known for bringing a very human and creative approach to security awareness. Why does that matter in healthcare?

Gary S Chan (14:43)

When you work for an organization whose mission is not IT, people don't think about IT on a day-to-day basis. Everybody uses a computer, but they don't sit there reading about computers, IT, and those processes. Everybody is worried about patient care. Doctors are very busy people and are focused, as they should be, on patients - not on whether they clicked on a phishing link.

You really have to tailor your messaging to those people. And it's not just doctors. Other executives care about different things. The executive responsible for legal cares about certain issues. Someone responsible for HR cares about something different. Being able to communicate in a way that resonates with them personally is what gets it into their memory.

I can tell you all day long not to share your password. But who hasn't handed their phone to their kid, put in the code, and let the kid play games while they're shopping because they don't want the kid bothering them? This stuff happens all the time. If you make it personal and say, 'When you do that, here's what some kids have done - they've placed additional charges on a parent's credit card because they downloaded something from the app store,' or explain how an action could put something wrong in the patient record and affect patient care or reputation, then people may think, 'Okay, maybe I shouldn't do that.' If you simply say, 'Don't share your password,' how many of us have heard that, and how many of us have still done it?

David Hacker (16:31)

What have you learned about persuasion, trust, and communication that our Health IT vendor listeners could learn from?

Gary S Chan (16:46)

Building trust is super important, and the way to do that is to be honest about everything. No one is perfect, and I really never get a perfect security questionnaire. It just doesn't happen. Be honest and upfront, and most of the time they'll work with you. Very frankly, it is a lot harder for me to deny something, because as soon as I deny it I get 20 escalations, and that's even more paperwork. I actually don't want to deny anything. I want to work with you. I have no stake in whether we buy from you or not.

If you're honest and say, 'This is where we aren't great, but this is what we're going to do about it,' I can document that and it will probably be fine, as long as it's within reason. Or you might say, 'We do these things really well, but for this part you may need to invest a little more to do an additional thing.' That's actually fine, because now I can plan for it. We might have to talk about the money and figure that out, but at least I know. I'm not hit with an unexpected charge later because your solution caused 20 other things to happen that you knew would happen but I didn't know would happen because you didn't tell us. At that point we have a major issue because there's no money to solve it. We may have to turn it off, and then there can be a contract or legal dispute. Being honest is just a basic human thing to do, but it also leads to much better outcomes.

I used to wonder why big companies have salespeople dedicated to selling to organizations instead of just putting the product on a shelf. Having worked in this for more than 20 years, I understand that the reason is trust. I'm much more likely to go back and buy more products and accept a company's word when, time and again, that company has been honest. That has a lot of value. These companies sell more than one product,

and we're always going to need more of the same product or other products. That's really it: just be honest. It'll be fine.

David Hacker (19:19)

How has the explosion of AI changed the security conversation within your team and overall in healthcare?

Gary S Chan (19:30)

I mean, just about everything. We get a lot of security questionnaires, and I'm sure many other organizations do as well. I'm pretty sure a lot of vendors now use AI to answer these questions, and that's not great. It's not honest if we don't know what's real and what's not. It's really changed the calculation, especially if we find discrepancies between answers. Then we know not only that AI was used, but that the answer was wrong.

AI has also changed the landscape because it's incorporated into almost everything, and you're constantly updating and patching these systems. We can't necessarily put static controls around something that changes so rapidly. Every couple of weeks there can be a new iteration. So as a vendor you need a very good policy that you can articulate: explain the types of things you will and will not do, adhere to that policy, and proactively notify us if something materially changes. That's how we can collectively stay safe. AI has changed tremendously how we're able to do the assessment and what the assessment means afterward because of all of those changes.

David Hacker (21:06)

All right, Gary. We've hit the lightning wrap. I have just a couple of quick questions. First, complete this sentence for me: A Health IT company is not ready for a security review until...

Gary S Chan (21:22)

It has at least one dedicated security person.

David Hacker (21:27)

What is one positive sign that a vendor really understands healthcare security reality?

Gary S Chan (21:38)

It comes with a certification or some other documentation that they've proactively created and provide to all of their customers.

David Hacker (21:47)

My last wrap question: If you could give one piece of advice to companies selling into healthcare, what would it be?

Gary S Chan (21:56)

Tailor to your audience. Tell me the security stuff. Tell the operational guy all the functional stuff. Tailor to your audience. Don't just give me everything.

David Hacker (22:05)

Gary, this has been great. But before we wrap, one of the things that makes your work so unique is that you use mentalism to make cybersecurity memorable. Since so much of this conversation has been about getting security to actually stick with people, I thought it might be fun to give you a moment to show the audience what that looks like.

Gary S Chan (22:26)

Sure. Let's do something fun for your audience. If you're watching, you can see some of this on the screen, but if not, audio is fine too. Play along; it'll be a lot of fun. Let me load this now.

All right, can you see my screen?

David Hacker (22:48)

Yes.

Gary S Chan (22:50)

Perfect. Here we go.

In your mind, pick a number between two and ten.

Take that number and multiply it by nine to create a new number.

Take the digits of that new number and add them together to create another number.

Subtract five from that number. Remember this number. We're now going to convert this number into a letter. One is A, two is B, three is C, and so on.

You should now have a letter. Think of a country that begins with that letter.

Take the last letter of that country and think of an animal that begins with that letter.

Take the last letter of that animal and think of a color that begins with that letter.

Through all of those steps, most of you will have come to an orange kangaroo in Denmark.

David Hacker (24:17)

Wow. I don't know about the rest of my audience, but that was exactly what I had. Gary, that was really great. To me, it reinforces the point that security awareness is not just about giving people information. It has to be memorable enough that people act differently when it matters. I really appreciate your time. I love the mentalist component at the very end. It added something that I hope people will take away and remember about this podcast. Again, I really appreciate your time, and thank you very much for joining me on Rockin' HIT Sales.

Gary S Chan (24:57)

Well, thanks so much for having me, David. It's been a pleasure.