uberknowledge

Gary Hayslip, CISSP

The storytelling CISO who leads by example

Gary points out that a CISO's hardest job is to help executives understand the value of cybersecurity and shares that storytelling is invaluable in gaining trust and promoting understanding.

02:34 In a breach the CISO does not own 100 percent of the blame.

03:46 CISO's help manage risk, but they do not own it. Risk belongs to the company.

04:43 Companies are getting mature about dealing with risk, security is just another part of that.

06:13 Managing cyber risk is not a one-off, it's a life cycle.

08:03 One of a CISO's toughest jobs is getting executives to understand the value of what you are doing and spending all the money and resources on.

09:14 Take the security speak and put it in to stories that people can relate to. Use storytelling and laughter to win champions and support within the company.

10:14 Use storytelling to help the board see how security benefits the business. Share your strategies and forget the fear factor.

12:50 Vendors can use storytelling to build trust too, but they need to do their homework and get context to understand their customers.

16:36 The three-step process that smart cities can teach enterprise about security: assessment, remediation and enforcement.

17:34 Cyber is continuous, it's a life cycle, but continuous is hard for organizations because it requires resources.

19:52 Unfortunately, in many companies, continuous security is not considered the norm, instead they ride the ups and downs of incidents.

20:30 Cybersecurity is never done.

21:56 Management is servant-leadership. Don't just manage people, actually serve them, lead them, and mentor them.

24:11 Build training maps for your staff, so they can see where they are at and where they are going.

25:19 How to retain your staff: make it fun.

Ashwin Krishnan: [00:00:40] So we are at the UberKnowledge podcast again, and today's guest is Gary Hayslip. Now, Gary has a very rich and diverse background, so I will not even attempt to introduce him; I'll let him do that. But suffice to say, we have a ton of information based on what you've written and spoken about, and we'll dive right in as soon as you give the audience a little bit of your background, Gary.

Gary Hayslip: [00:01:05] Yeah, I've been in IT and cybersecurity for going on 20 years. I was active duty military, you know, working in those fields in the federal civil service for the U.S. Navy as a CIO and CISO. Then I was the CISO for the city of San Diego and the CISO here at Webroot. Webroot just got acquired, so I'll be moving on to my next role, once I figure out what that is. I've worked extensively in IT and in cyber, IoT, smart cities, you know, a wide range. And again, as you mentioned, I've helped write books and articles on everything from managing security teams and building out security programs to threat intelligence to smart cities, so a little bit of everything. I'm kind of one of those people where I find technology, especially cybersecurity, fascinating. I'm very curious, I'm constantly breaking things and looking at things and trying to figure out, how do we do it this way and what happens with this. And so I definitely am not bored any time soon. I love our community, and I love to see what startups are doing and what people are doing with technology.

Ashwin Krishnan: [00:02:33] So that's a great introduction, when you talk about the need to break things and look and figure out the reason behind the why. So one particular article that caught my eye, and I believe you posted this on LinkedIn, talks about the CISO manifesto, recruiting CISOs not unicorns. It's a very interesting and informative set of frank guidelines. There's one I wanted to particularly call your attention to which is security is never 100 percent. So in the event of a breach, the CISO does not own 100 percent of the blame; manage the incident and learn from it instead of killing the messenger. Now this is such a powerful statement. And I have heard very few CISOs stand up and talk about it in such honest terms. So what prompted you to write this and more importantly what would be the measure of success? Is it a realization for the ecosystem that a CISO operates in to realize that the board cannot hold only them accountable? So, what is the motivation, and what value do you think this provides to the reader?

Gary Hayslip: [00:03:47] Well, you know, the biggest thing that actually is tied into another thing that I had added and that was the fact that when you look at it CISOs, if you're in that role as a chief information security officer, I look at the fact that you're really a business executive just like any other in the organization, except that you use technology, people, processes to manage enterprise risk. Yes, you're helping manage companies' risk. The thing is that you don't own that risk. The risk actually belongs to the company. And the reason is

> "You don't own that risk. The risk belongs to the company."

that risk is business decisions, it's decisions that they've made on technology or decisions that they've made with DevOps or decisions that they've made with new products. And your job is to understand that risk and help them see it and figure out what is the mitigated or accepted level and manage it.

[00:04:43] If you have a healthy discussion and relationship around that and the management of risk, then when it comes to breaches because they're going to happen, nothing is 100 percent; I know vendors like to sell that, but that's crap, nobody's 100 percent. And so what you can do instead though is that if you have, as a security executive, as a CISO, if you have a healthy relationship with your leadership team, if you have a healthy relationship with the culture itself within the business, you can help the organization be resilient. You can help them go ahead and put a security program in place and controls. You can do planning and training in regards to incident response, so when incidents do happen they don't have as large of an impact; they don't hurt the customers; that business doesn't go down. You can absorb that breach and still be able to manage customers and still be able to do your job while you triage it, clean it up, learn from it and go on about your business. And so for me that whole thing was helping companies understand that you're getting very mature about how to look at risk, well this is just another piece of it. And stop going and paralyzing the CISOs. They're scared to death, and they're dealing with all this and everything else. Breaches happen.

Ashwin Krishnan: [00:06:12] Yeah.

Gary Hayslip: [00:06:13] They're a part of business. Now, with that said it doesn't mean you should just accept it and say, "Hey, we're just gonna go ahead and get hacked." No, you can go ahead and be mature about it and put the controls and the program in place and manage your risk, so you can reduce that as much as possible and you can be resilient, you can be flexible, you can be nimble. And that's my thing, I'm basically a systems thinker; I look at these as pieces that are tied together. I try to get my executive team to understand that it isn't a one off, it's a life cycle. These pieces have to come together, so we have not just a healthy security program, but we manage risk healthy as a business.

Ashwin Krishnan: [00:07:03] Amazing articulation! I wanted to also touch upon something else, which I've never, never heard any CISO talk about. This was one of your Forbes articles that you authored, I believe late last year, where you talk about laughter and storytelling as key tools to help you be an effective CISO and relate why change needs to be made. I could not agree more myself on this. It's storytelling as you talk about expressing ideas through emotion to persuade an audience to learn about a causation. And giving them something that they can relate to in their own life and then they become not just a passive participant but an active instigator. So clearly, based on your article, you've been using storytelling very effectively. This is so fundamental, so basic, do you see other CISOs doing this?

Gary Hayslip: [00:08:03] One of the things I go ahead and I talk about is that as a

CISO one of the hardest jobs that you have is trying to get people to understand what's the value of what you're doing and for them to be able to see the value of spending so much money and resources and everything on a security program.

[00:08:20] I used to joke that five years ago security was kind of in a box. We were in the back room and people didn't know who we were. Now all of a sudden, you're expected to be a business executive and supposed to be supporting the business, but a lot of us don't know how to do that. I find that one of the biggest barriers for me as a CISO to be effective but also one of the biggest assets is business culture, the people — the employers, and the employees around my team, the people that we're actually supporting, our customers — and a lot of times, they don't really understand what we're doing or don't really understand how we're there to support them.

00:09:14] What I found is that to get the culture behind us and support us and get champions, there's times where you have to be able to take all the security speak and put it into stories put it into things that people can relate to. Put it in the things that make sense to them, so they can see not only how it makes sense for them when they're at work, but also when they're at home and their kids are on their computer and something gets infected on their cell phone. One of the things I talk about in that article also was not just using storytelling and laughter, but the fact that using those and being able to understand the audience that you're speaking to, which one you should use so you can build trust, so they can get used to working with you and trust your teams and understand that OK this is the value that security is supposed to be bringing into the business.

"Take all the security speak and put it into stories."

[00:10:14] I talk a lot about the fact that CISOs when they're dealing with leadership teams, when they're before boards there is this whole aspect of telling a value story, of relating that "OK, I don't generate revenue, but I enhance the company's ability to generate revenue and do it safely," and a lot of that is storytelling. Yeah. And you know I find guys that ... you can't do the old, let's scare them to death, the sky is falling and you've got to do this — no! We talk about these are the risks that we have, current state. Here's my strategic plan over the next three years. These are projects that I want to work on. These are the new business services that we can put in place or ones that we can enhance and make better. You know with these resources you're telling a story that they can relate to, especially when you're talking to a board, you know, business-orientated people, they can see how this is going to help the business.

[00:11:20] I had spent time with a couple of long-term CISOs and CIOs who were mentors of mine when I was in the military. And I was fascinated with the way that they could do that, with the way that they could get an audience to relate to them so that they could use that trust and that culture within the business to get things done.

Ashwin Krishnan: [00:11:48] Yes, I was going back to the same article, and you already mentioned this in the response, but for the purpose of the listeners I want to call out this formula, which I think is absolutely amazing: context plus value equals informed decision making. And this is kind of what you were talking about, build the context so that the audience understands in their own terms what this means, and then what's in it for me, which is the value, and then they end up taking a decision.

[00:12:16] So, turning the question around to vendors: if you've made this a part of your ethos and you've successfully been able to convince your peers and the board that you report in to, would you say vendors should adopt the same formula? So instead of coming and trying to sell to Gary, like you said using FUD, which clearly doesn't work anymore, but does the same "context plus value equals informed decision making" apply when vendors come and peddle their goods?

Gary Hayslip: [00:12:50] I honestly think so because my thing is that the context piece is getting the know the person that you're coming to sell to; not only getting to know them but understand the current business culture that they're in, understand the issues that they're having and the problems that they're trying to solve. Understand that the problem that you're trying to solve, that you are there to fix, may be really low on their priority list because they've got two things that are clearly on fire that they have to manage. Know those things, then you're not going to go in there and try to waste their time, thinking they are going to purchase your product because it's just not going to happen. They're extremely focused on something else. If you have that context already, you know when to approach them and how to approach them, and it also shapes the value story, it also shapes how you lay it out for them, so it relates to their needs.

"The context piece is getting to know the person that you're coming to sell to."

Ashwin Krishnan: [00:13:55] That trust that you talk about, which is if I'm trying to sell something and you're saying it's in probably the bottom five, but your house is on fire and you have the top three, would you as a CISO give that information out to vendors or would you only do that with vendors who have built trust? It's a catch-22 situation right, where let's assume I'm a vendor trying to sell Gary something, but I will definitely not sell it to you or I will try to put it in context if I know that you have priority one, two, and three, which really doesn't directly fit. But how does a vendor actually get hold of this information, so that they can do the right thing to be able to build a context around how they can or cannot solve a problem?

Gary Hayslip: [00:14:44] For me, background information is something that I would give out to someone I trust. Sometimes that might be fellow CISOs — we're on a roundtable, we're talking with each other, and we're trying to help each other. It

may be fellow CISOs that I'm on a Slack channel with, and we're sharing information back and forth, and again, trying to help each other. It all really depends, you know, where you would get that kind of info. If you just blind call me ...

Ashwin Krishnan: [00:15:22] [Laughs]

Gary Hayslip: [00:15:23] I have no idea who you are. I don't even know if you're a cybercriminal or a real salesperson. I'm not going to go ahead and share, especially on LinkedIn. If you do the whole, "Hey, let's connect," and then you turn around and try to sell me something? Yeah, I'm immediately going ahead and reporting you for spam and blocking you.

[00:15:46] What I have found, for those salespeople that have done it really well, is they know what professional organizations I'm a member of, they know I go to the lunches, they know I participate in the community. They tend to meet me at those type of events; where we can meet and talk face to face. If I'm able to talk to you face to face, I will let you know this is what I'm working on, this is what's important to me right now.

Ashwin Krishnan: [00:16:18] That's I think a great insight into it because that's probably one of the hardest things vendors struggle with. But the stuff that you mentioned about cold calling and using LinkedIn as a "lead gen" typically that does not work.

[00:16:36] So you mentioned you were CISO of the city of San Diego. And there was an article that you authored when you were spearheading that organization which was about how smart cities can teach enterprises about security. You called it a three-step process, which I'll just articulate here for the benefit of our listeners. Number one, assess your network by adopting a security framework such as NIST or CIS. Identify the networks that had some gaps and determine which policies, procedures, and solutions you need to adopt. Number three, create a comprehensive security program that gives you a holistic view of the overall IT environment and the ability to continuously monitor for vulnerabilities. Now this looks, on the face of it looks, extremely straightforward, but clearly many, many organizations fall short. So in your view, what is it that prevents organizations from embracing such a closed-loop assessment, remediation and enforcement.

Gary Hayslip: [00:17:34] Honestly, I think one of the biggest issues — and this isn't just for cities, this is just organizations in general — the problem is that you get this road map and you're like, "I got this, I can do this, this, this, and this. I got this check sheet, let's go," and they forget this is continuous. I mean, I've had to explain to security execs, I've had to explain to the CEO several times, I've been invited by fellow CISOs to come in and help them present to the board, and

"You start this process, it's continuous, which means you have to give it resources."

I've had to explain to them several times that cyber is a life cycle. You know, you start this process, it's continuous, which means you have to give it resources; the teams need to be managed; the risk needs to be managed — continuous monitoring.

[00:18:25] I honestly think what happens is that we do really good at the beginning, and then, as we get in when we get in and get the program up and running and we're doing well, people leave. New people come in, the program ages over time, and we kind of slough off, things fall between the cracks. Then every once in a while, you'll have an incident or something like that, and we stand back up and let's do this better next time, and you know, we do that for a while and then ... it's cyclical and it's up and down. It's very hard for organizations to be continuous all the time. You know, that requires money, that requires resources, that requires the right people, that requires a business culture that accepts security as a core business tenet of how they compete. It's just accepted that this is one of our strategic values that we're going to fund and manage, and we use cybersecurity to do the rest of these things well. You know, some businesses accept that, and they really, from a leadership standpoint, put their money where their mouth is, and the rest of the culture, the rest of the organization accepts it and it becomes the norm.

[00:19:52] You know those companies are very mature, and I've seen companies like that where security is considered the norm. And if you're not doing it, everybody's just looking at you like, "Hey, this is how we do this around here. What are you doing?" Unfortunately, that's not the norm, and instead it's more of the cycle where you go up and down. A lot of times when you go down, you have a breach or you have an incident, and then you go back up for a while, and then you go down you go back. I do think anything that's continuous, honestly from a business perspective, sucks. People don't like that. What they're looking for is, "We're in a tunnel, and there's a light at the end of the tunnel, and woo hoo, we're going to be done." That's not cybersecurity; cybersecurity is never done.

Ashwin Krishnan: [00:20:44] Actually that's an important point because you're right. There's usually a lot of furor and enthusiasm when you start a new initiative. But then once it gets to continuously needing to keep up with it, people lose interest and that's where a lot of those challenges happen.

[00:21:19] So Gary, moving on, I know we are running out of time, but I want to touch upon one last thing which is the issue of diversity or rather lack of it. I'm not just asking the question when it comes to the number of women in cybersecurity, which is clearly abysmal, but also the Gen X, Gen Ys, Gen Zs, the new generation, if you will. How they think about security, and how do you recruit them, attract them to join an organization? So, what are your views? I know you've done this successfully for many, many years, over many organizations. What has been your formula to make sure that you have a diverse workforce? Number two, how do you make cybersecurity a mission and get people as interested as you are after

many, many years to stay on top of it, knowing that this is an ongoing battle?

Gary Hayslip: [00:21:56] For me, I've always approached it as a servant-leadership thing. I was trained in the military, and my job is to not just to manage people but to actually serve them and lead with and mentor them. Every place I've been, I've had people that have followed me from company to company because they want to work for me. I've had young people, men, women and a mixture of everything; I've always had very diverse teams.

[00:22:35] I look at it as security teams are very close knit. We work with each other 24/7. It is very critical that you get people with soft skills that understand how to be able to work with each other and not get on each other's nerves. You know I've been in teams where people want to strangle each other because they just can't get along at all. And so, I watch for that. But at the same time, I want to learn and get to know my team members. I want to learn and get to know how to fit them in different projects. What I do a lot of is I assess each of them, so I can better understand their soft skills and their skill sets, their experience, their education, what certifications they have. I actually build out training maps for each of them, where they're at in their careers. I seek to help them professionally. So they're working on something professionally, but then they're also working on something project-wise or hobby-wise to help them grow within the field. And I constantly check on them to see how they're doing. And then I do it myself. I hold myself to the same standards. So they can see that I'm actually involved in the community, and I'm actively educating myself and working on things.

"I hold myself to the same standards"

[00:23:52] I've done everything from bringing my whole team with me to Black Hat and DEF CON, so we spend time together. But even while we're all there together, somebody is monitoring our inbox. Somebody is responding to tickets, just because we're at DEF CON doesn't mean that we don't take care of our customers.

Ashwin Krishnan: [00:24:10] Right.

Gary Hayslip: [00:24:11] What we'll do with the teams is everybody is assigned, each member of the team is assigned a couple of different technologies in the security stack. So everybody has responsibility for something, and then they get trained and cross trained on different pieces of that stack. They get trained professionally for a specific certification for where they should be at within their profession; whether they're an analyst or they're an engineer or an architect. And then at the same time, I'm looking at ... I kind of roll these together, and I'm looking at them across the board as a person, as a team member, and then as a future executive, you know, where they're gonna be at. I spend time with them in one-to-one meetings to find out are you interested in being a future CISO, or do you just want to be an architect? You love doing the technology stuff, but you really don't want to deal with executives. Yeah. Which I can I can sympathize with, there

are times when I don't want to deal with executives.

[00:25:19] But that's a lot of what I do. I find making it fun, giving them a roadmap and a path, so they can understand where they're going, helping them understand that this may look like a long path, but don't worry about it, let's break it down, focus on small pieces, one at a time, and that's all you've got to do. One step at a time. Also emulating the same thing that I'm expecting them to do, so they can see how it's done. Giving them the ability to be able to reach out to me, so we can adjust their path, adjust their career map, if they want to make changes. But you know each of them has one, so they understand where they fit in the overall team, but they also understand where they fit in their own professional careers.

Ashwin Krishnan: [00:26:04] That's great advice, just broken down into digestible chunks, so that people don't feel overwhelmed saying, "I'm going from point A to Point B, but what are the steps?". The other piece that you mentioned, which I think is really telling, is doing it and showing the way. It's one thing to stand up as a manager and say, "Hey thou art to do this," and you continue doing what you're doing, but in your case, clearly, you're walking the talk, which I think is obviously very inspirational.

[00:26:34] So Gary, again I thank you for your time, I know we have scheduled this in short order, so I wish you all the best in whatever your next role is. Looking forward to chatting with you in the future as well.

Gary Hayslip: [00:26:48] Thank you very much. Definitely reach out; I'd be more than happy to come back.

Ashwin Krishnan: [00:26:53] All right, thank you, Gary.

Gary Hayslip: [00:26:54] Thank you. Bye bye.