Bonus: Cybersecurity Canon Hall of Fame interview with Caroline Wong on "Security Metrics: A Beginner's Guide." TRANSCRIPT

Rick Howard: You're listening to the theme song of the HBO long-running hit "Game Of Thrones," the unofficial anthem for the Cybersecurity Canon Project, the project designed to find the must-read books for all cybersecurity professionals because one of the greatest characters of all time, Tyrion Lannister, had this to say about reading books.

(SOUNDBITE OF TV SHOW, "GAME OF THRONES")

Kit Harington: (As Jon Snow) Why do you read so much?

Peter Dinklage: (As Tyrion Lannister) Well, my brother has his sword, and I have my mind, and a mind needs books like a sword needs a whetstone. That's why I read so much, Jon Snow.

Rick Howard: Which means it's Cybersecurity Canon Week here at the CyberWire, where we are interviewing all the Canon Hall of Fame inductee authors for the 2022 season. I'm Rick Howard, the chief security officer, chief analyst and senior fellow at the CyberWire, and today's book is called "Security Metrics: A Beginner's Guide" by Caroline Wong. Enjoy.

Rick Howard: I'm joined by Caroline Wong, the chief strategy officer at Cobalt and host of her own podcast, "Humans Of InfoSec." Caroline, thanks for coming on the show.

Caroline Wong: What a pleasure to be here. Thank you for having me.

Rick Howard: You're quite welcome. So you wrote this book in 2011, and as near as I can figure, it's one of the first books published for the cybersecurity community that dealt with the thorny subjects of risk, metrics and analytics. Why did you write the book?

Caroline Wong: So first, I have to say, Andy Jaquith...

Rick Howard: Yes.

Caroline Wong: ...Wrote a super good book about security metrics before this book. I was so honored that Andy wrote a little bit in this book as an introduction. I certainly want to respect the shoulders of giants that I stood on in order to produce this work. Andy had done excellent work in this area. And what I had an opportunity to do was to say, how do you take some of these really great ideas that for the most part, at that point in time, now more than a decade ago, were largely theoretical, and how do you put that into practice? And that's what I was very interested in doing.

Caroline Wong: I had the privilege of working with Dave Cullinane when he was CISO at eBay. And together, we and the team - we built this program, and I saw the value and the necessity of security metrics, not only to demonstrate the value of the program, but also to ensure ongoing investment. And it's a topic that has fascinated me throughout my career.

Rick Howard: Well, Jaquith book is one of the first books that was submitted as a Cybersecurity Canon Hall of Fame candidate. I think I even wrote the book

review for that one, so I'm happy to hear that you took what he did and took the next step. And I want to personally thank you for taking some time to explain some things to this lowly CISO who doesn't have the best math skills in the world. Like the difference between analytics and metrics - can you just tell our audience what the difference between those two things are?

Caroline Wong: So numbers in of themselves are not, in my opinion, that valuable. In order for us to learn truth and wisdom and even to receive information that might help us to answer questions, that might help us to make stronger decisions, that does require analytics. Typically, we're not talking a single number. Typically, we're talking a trend line over time, maybe a ratio because I do think that security is a super difficult field to measure.

Rick Howard: It really is.

Caroline Wong: You know, and since the time this book was published, certainly there have been a number of brilliant folks who've also written about their thoughts on it. And I think fundamentally, the reason it's difficult is because it is really hard to pin someone down and get them to explain what their risk tolerance is. And the thing about risk tolerance, you can't simply say, hey, Rick, what's your risk tolerance on a scale of 1 to 10? That's not how these things work. At the end of the day, the conversation needs to be not only what do we as an organization believe our risk tolerance should be for this specific business that we're doing, and then what is the appropriate amount of investment that one puts into an information security function in order to achieve alignment with that risk tolerance? Numbers can help, and numbers are part of the equation, but numbers are not all there is to it. There's so much to do with effective communication and context setting, which is another way of saying analytics.

Rick Howard: Why I totally agree with you - right? - because risk tolerance, as you say, is different in every organization. It's based on a number of factors - not just numbers, like you were talking, but also on the culture of the company and the risk profile of the leadership. A 20% probability of a material impact to one organization might be OK, you know, in their risk tolerance, but it might be run around with your hair on fire with another organization because they couldn't stand it. It all depends on the leadership and the culture and the numbers you provide them. Is that what you're saying?

Caroline Wong: Absolutely. The thing about security is that security is about protecting value. Today, in our modern world, so much of what we value has really changed from being something physical to something digital. And so value creation and therefore value protection happens with regards to software and the internet and data and information. And so we have an opportunity to say, well, how do we think about risk? How do we want to not only think about but put into action what we think about risk? And this is very specific to an organization's business model, what an organization considers to be critical and a number of other factors, including things like, how does this particular organization do security testing? What methods are they using for defect discovery? What is their technology stack? I mean, endless questions that have everything to do with the uniqueness and the specificity of a particular organization. A decade ago, I worked with a large group of volunteer industry folks. And we worked with CIS to put together sort of a top 10 list, if you will, of security metrics. You know, that was not a bad project. But the failure of that project in concept is that it's different for everyone. And the challenge and the fun...

Rick Howard: Are you going to give me the, it depends? That's what everybody says - it depends - because it's totally true. It depends on your situation.

Caroline Wong: It does depend.

Rick Howard: (Laughter).

Caroline Wong: And I'll tell you what. I'll say it depends. And I'll also tell you that I have an idea for a starting point. And this idea is not my idea. This idea is Sammy Migues' idea. I had the great privilege to work with Sammy Migues. We were both working at Cigital a few years ago. And there is this concept, which is risk management objectives. And fundamentally, the idea is a security leader could talk to a business leader and say, hey, let's find a place where we have common ground. Let's try to identify a shared goal. Let's get really specific about that objective. And then I will go off and make a plan to achieve that objective. And I will keep you updated. And so, for example, some of those common shared goals between security folks and business folks might be, hey, we want to use cybersecurity as a competitive differentiator. We want to comply with some regulatory requirements, some contractual obligation, some industry standard. We want to achieve a defensible level of due care. They get a little more interesting than that because those are all sort of basic in my opinion.

Caroline Wong: But here are some that I think are really interesting. Hey, we want to prevent the same cybersecurity problems from happening over and over again. Hey, we want to reduce the probability that malicious attackers can stop critical systems and applications from functioning. Hey, we want to require fixes for security bugs for which well-known attacks exist. And another really common one, hey, we want to achieve a comparable level of cybersecurity to our peers and/or our competition. And these are just seven statements. But I think that they are both sufficiently broad that they make sense to everyone, as well as sufficiently specific that you could say, okay, if we agree to this, then I can go and put together a plan. And I can tell you how

much that plan costs. And I can implement that plan, and we can actually measure progress against this plan. So to date, after more than a decade of thinking about this and talking to a bunch of folks about it, I think this is not a bad way to go.

Rick Howard: So I'm going to get to risk in a second. But before, I forgot to tell you that first, thank you again because for the first time in my career, I understand what a whisker chart is - all right? - and how to read it, what linear regression is and how to easily build plots with the data in a spreadsheet. And I actually did some practice runs because of your book, Caroline, in Google Sheets to see if I could do it. And I'm here to say if I can figure it out, I think anybody can do it thanks to your explanation. And the last one is exactly what is logarithmic scale and why mathematicians use it. So just, you know, as an example, can you tell our listeners, why do we use logarithmic scale in metrics and analytics?

Caroline Wong: Sure. So, gosh, these math things, these modeling things - they are tools for us to use. You know, they are not by any means the end result. You know, I think the simple description of linear versus logarithmic - you know, it's kind of like the earthquake scale. You know, what's the difference between a size 7 earthquake and a size 8 earthquake? If I ask my 7-year-old daughter, what's the difference between the number seven and eight, she says, that's not a very big difference. You know, seven is followed by eight. But if we're talking about logarithmic terms, then we're talking about a magnitude increase times 10. And so it's, like, just way bigger. And so it just depends on your dataset. It depends on the velocity at which your data is changing whether it's useful to view it in a linear or logarithmic fashion.

Rick Howard: Thank you for that explanation. I appreciate that.

Caroline Wong: (Laughter).

Rick Howard: So let's get back to risk for a second. One point of clarification, in the book, you say that as security professional - I'm quoting here or paraphrasing here - as security professionals, we are in the business of reducing cyber risk to a level that the company leadership is comfortable with. I love that statement. I absolutely agree with that. But then you say that this is not always easy to achieve quantitatively, that qualitative judgments with respect to risk reduction are useful during prioritization exercises, which I admit sounded odd, especially in a book about math and metrics. And even you acknowledge that in the book - that you say that not everything is about the numbers. I just wonder if you want to elaborate on that a little bit, and what were you trying to say there?

Caroline Wong: Yeah. You know, I think the thing about risk management is, you know, it is obvious to so many of us that you should not try and protect a $5 asset with a $200 fence.

Rick Howard: Indeed.

Caroline Wong: And I think where a lot of the challenge comes in is that where a company executive may have their risk tolerance, a lot of times, the security leader has their risk tolerance in a different place. A lot of times, the security person does not agree. Sometimes the security person does want to put a $200 fence around a $5 asset when actually, that may not be appropriate for the organization.

Rick Howard: Well, I was talking to a friend of mine - actually, he's my next-door neighbor. He's a CSO of a big company here in the Virginia area. And

he has a very large program on insider risk. And I was asking him, well, how often does some insider risk thing happen that causes the company material impact? And, you know, he doesn't have one - right? - and I'm saying, well, that seems like you're spending a lot of money on something that doesn't happen that often. And he goes, yeah, I know. He says, exactly what you said. I spent $200 for a fence for a $5 item.

Caroline Wong: The thing is that as humans, I think the risk management can be so personal, and it can be so emotional.

Rick Howard: Yeah, that's true.

Caroline Wong: So we have these psychological things about the way that our brains work. We are, for example, susceptible to marketing. And maybe this CISO or that CISO has heard a really good pitch recently, and they think, wow, that sounds very interesting. Interesting is not always the same as impactful.

Rick Howard: Yeah.

Caroline Wong: I actually think that some of the most important things that need to be done in our industry are really basic, really fundamental and kind of boring. You know, if you look at ransomware, for example, in 2021, ransomware is all the rage. 2022 ransomware is all the rage more so. Ransomware is a service. When was the first ransomware attack?

Rick Howard: It was, like, early 2000's - right? - something like that?

Caroline Wong: Oh, my gosh. Get this - the first ransomware attack happened when I was 6 years old.

Rick Howard: (Laughter) That's excellent.

Caroline Wong: And I'm about to be 40. And here's what that means - it's not new. And in 2021, we find in the United States that our food supply has been hacked, that our energy supply has been hacked. And what's so crazy about all of it is that we, as cybersecurity practitioners, we actually know exactly how to prevent and eliminate ransomware. You simply have to know your assets, backup your data, test your backups, and make sure that your software is up to date and patched, and that when you find security vulnerabilities, you fix them. It's actually simple. It's not easy. And frankly, it's not that sexy or fun, right?

Rick Howard: It's meat and potatoes, meat and potatoes kind of stuff. Yeah.

Caroline Wong: Right. When was the last time you went to a company meeting and the CEO is raving about making sure your backups work?

Rick Howard: (Laughter) That's right. It's...

Caroline Wong: And my hope...

Rick Howard: ...You're right.

Caroline Wong: ...Is that security metrics can help us point in the right direction. Sometimes the things that are important and impactful are boring, and that doesn't mean you shouldn't do them. And maybe we can use data to point us in the direction of, OK, if we think through where we're spending our money, are we actually spending our money on the relatively high-probability, high-severity items, versus how much are we spending on the relatively low-severity, low-probability items? Because I just heard a really good marketing pitch or because I'm an engineer, and I think this thing is, like, flashy and shiny. I think that we as an industry have an opportunity to really evaluate our problem statements and try to act based on trying to solve those problem statements rather than, you know, getting really overly excited about sparkly stuff and then chasing it and trying to put solutions onto things that aren't even broken because it's fun or cool.

Rick Howard: So the book's over a decade old, and the thinking on this subject has evolved since then. We've had other authors entered into the fray, like Dr. Ron Howard and Freud and Jones and Tetlock and Hubbard and Cyrus and, so if you're going to write the book today, Caroline, what would you want to be putting into it that wasn't - that you didn't have, you know, when you wrote it over a decade ago?

Caroline Wong: So funny and fun to reflect on the time that's passed. When I wrote the book, application security was like the cutting edge, all the rage, you know. And cloud security was something that was not normal yet. It wasn't mainstream. And here we are. You know, I think that one of the things that was somewhat true at the time, but is way more true now, has to do with the interdependency of software companies. So if I take Cobalt as an example, we're an organization. We've got thousands of customers. We've got dozens of software vendors. Every organization that is a software organization relies upon a bunch of other organizations that are software organizations. And therefore, my partner, my vendor, their security profile has an impact on my

security profile. We are not isolated. We are not islands. And this is something that I think if I were to write it today, would be deserving of some focus and some attention.

Rick Howard: That's Caroline Wong, the latest author inductee into the Cybersecurity Canon Hall of Fame, with her book "Security Metrics: A Beginner's Guide." For more information on the Cybersecurity Canon project, go to your favorite search engine and look up Cybersecurity Canon - that's canon with one N, as in canon of literature, and not two N's, where you blow stuff up - and Ohio State University, the project's official sponsor.