uberknowledge

Malcolm Harkins,

Chief Security and Trust Officer, Cymatic

The Human Element: Cybersecurity's Weakest or Strongest Link?

Malcolm talks about the people perimeter, simplifying to manage risk, and trust as a function of competence and character.

03:58	Humans are a weak link and a strong link. Don't blame the end user.
05:11	It is possible to change end-user behavior.
08:55	Simplify because complexity increases risk.
11:49	Roundabouts can teach us how to present information and manage risk.
16:26	Trust is a function of two things: competence and character.

Ashwin Krishnan: [00:00:43] So welcome to Cyber 360+, another episode of the UberKnowledge podcast. And I have, for the third time, Malcolm Harkins joining us. Malcolm, you've obviously gone through a big change in your career. Talk to the listeners about that, and then we will dive right into the people angle of security.

Malcolm Harkins: [00:01:06] Thanks, Ashwin. Yeah, happy to tell folks about the change that I have gone through. The week before Black Hat, I announced that I had joined a very early stage startup called Cymatic.io. Cymatic focuses on mitigating and managing risk prior to people gaining access to websites, web apps, web services, either externally or in the internal use case, by giving you better confidence in the device, in the state of the device, whether or not it is vulnerable. Not just confidence in the credentials being used by whoever's attempting to gain access and whether or not those credentials are potentially vulnerable, but also giving you confidence in who or what is behind the keyboard by what we can do with mouse movement, keystrokes, misspellings, and those type of things. So, I'm hugely excited about it, and it's going to be a fun journey. I'm jumping in and creating policies all over again and starting to build an internal security and risk and corporate social responsibility program and privacy program to make sure we've got our own internal stuff right, while we are trying to help protect our customers.

Ashwin Krishnan: [00:02:36] Excellent. So that segues beautifully into the topic of today, which is the human being. Typically, we hear about humans being the weakest link, but I wanted to bring to your attention the converse of that: humans being the strongest link. The latest one that I was reading about is Isaac Badu of Lubbock County, Texas, who apparently saw some icons being restructured or moved around on his computer and quickly alerted the team. They got the forensics involved and literally were able to stop the ransomware attack. So that for me was like, here is a human being actually doing the right thing and successfully stopping an attack.

"We hired smart people, sometimes they just made poor decisions."

[00:03:26] So just talk a little bit about your experience both on the customer side, the awareness, but also on the vendor side. Given that you've had the luxury and the good fortune of being on both sides, where is the human being in this mix of things? Do we continue to say he or she is the weakest link, or is that changing? Is there a different lens we need to look through at this carbon lifeform?

Malcolm Harkins: [00:03:58] Well, I think both are true. Dating back into my Intel days, back in the early 2000s, I was one of the earlier corporate security heads that started spending a ton of money on end-user training and awareness. I believed that what I could do was make them smarter; we hired smart people, sometimes they just made poor decisions, and sometimes those poor decisions then affected risks. But what I never wanted to do, and I don't believe that we should do, is blame the end user because when an end user does something, they click on a link, they open an attachment, they use their username or password to log into things and bad things

happen, that's a technology failure. But technology is managed by, guess what, people, and security professionals are, guess what, people. And so actually, in both of my books there's an entire chapter dedicated to people at the perimeter. It talks about the people perimeter and what we should be doing to grow that.

[00:05:11] Much like the example you gave for Lubbock County, I had a similar incident back at Intel after I'd spent millions doing training and stuff like that. This was a time, and I actually think I articulated in the book that, people were starting to question my spending on end users and their awareness of things to mitigate risk. And one time, the H.R. team had decided to hire an outside firm to assess whether or not the company was a great place to work. And they worked with the messaging team to make sure that the message coming from that outside firm was not going to get blocked by the spam filters, but the security team wasn't aware of it. And I had been doing this awareness now for years in poster form, videos, email messages, different things in different mixed media to get people to generally be cautious of things that would come through. And as soon as that survey hit, it went to a random 10% of the population at 4 p.m. Pacific Time, to hit end of day in the West Coast, but also APAC and stuff like that, within minutes, the Help Desk started getting crushed with calls from employees thinking we were under attack.

[00:06:32] My team activated immediately to cut the messages, start rolling it back from anybody's inbox who had gotten it. We went full-tilt emergency response. 15 minutes later, one of the directors in the Human Resources team who led the survey is calling my cell phone, saying you just screwed up our corporate survey of employees. And I had proof for the first time, I had statistical proof, that I was able to change employees' behavior. I said, "You know what, I just spent a lot of time and effort to cause people to be cautious of external things that didn't seem like they came from us and stuff like that, why didn't you have the head of HR send the email?" And they were like, "We didn't think about it." So, I had my proof that I could change end-user behavior. I believe that we need to do that, but we also need to change the behavior and the human element and the creators of technology and the decision makers around risk, because that's really the human issue that we've got.

"I had my proof that I could change end-user behavior."

Ashwin Krishnan: [00:07:39] Yeah. You bring up a really interesting concept called the people perimeter. So, Malcolm, the perimeter is constantly changing, right? Obviously, in your 17 years at Intel, there were clearly many major initiatives that you would have undertaken, as would the CIO and lines of businesses, in terms of bringing new technology. So, there are traditional phishing attacks and other vectors, but those are constantly changing. How does an organization deal with the issue of, it's not just a one-time training? Like you said, you obviously employed a variety of means to keep people engaged and active, but that's a rarity, in my opinion. It's usually a checkbox item. People are trained once a year and then everything is good. That clearly doesn't work. So how does somebody reconcile themselves to saying, OK, people have legitimate work-life objectives to run, but at the same time, the attack

vectors are changing, there are new initiatives bringing in new threat vectors, be it cloud, IoT, or anything else, so how do you reconcile the too much information, changing perimeter, and people really having less and less time to do their daily job?

Malcolm Harkins: [00:08:55] You've got to get back to simplicity because complexity adds risk. If we do a lot of complex things to educate the users and stuff like that, we will confuse them or they'll ignore it. You know, the prior couple of years at Cylance, we got creative. The typical computer-based training stuff, it kind of gets boring after a while, so we did escape rooms, and we created an escape room for the annual information security training. Guess what? Every employee liked it. I'm in a security company with a bunch of hackers, right, and we did rudimentary awareness training to create an escape room and the employees loved it. So, you got to get creative.

[00:09:44] The other thing is, and you go back to the human element, and I've stated this for a long time and it's in some of the things I've published and talks that I've done, the biggest vulnerability we face today and in the future is the misperception of risk. Users misperceive it, decision makers misperceive it, the security team misperceives it. What's the mitigation for the misperception and what's the cause? Well, the cause is economics and psychology.

"The biggest vulnerability we face today and in the future is the misperception of risk."

[00:10:08] On the psychology side of it, if you believe in the benefit of something, you know, you're chasing the shiny bauble, you psychologically start discounting the risk. We have to figure out ways to mitigate that. And on the economic side of it, some of it is driven by, you know, moral hazard issues, the economic principle, that it's somebody else's risk, not mine. And so, you get different behaviors. There's a quote — and I like quotes, you've probably heard me say a few of them — the guy who created the Deward distillery had this quote that said, "Minds are like parachutes. They work best when open."

Ashwin Krishnan: [00:10:53] That's a good one. I'm going to use that.

Malcolm Harkins: [00:10:57] When you think about it, you go, how do I get people to not misperceive the risks; how do I get them to think differently? Now again, go back to my Intel days, the early advent of social computing and stuff like that, and Intel was doing wikis and internal blogs and stuff all before Facebook and LinkedIn and all this stuff blew up. But we could see that stuff coming, and I told my security team with the concept of people are the perimeter because guess what, the person is where you're making the decision. The person is where computing happens or it's going to be with them or on them or in them in the future. So truly, it is the person who is the perimeter and whatever device or application they have with them or they're accessing, but how do you cause them to have an open mind?

[00:11:49] And so I have this theory with social computing that I think worked relatively well, and I still approach some controls this way. It dated back to my time in undergraduate when I did research and transportation economics. What's the most effective and efficient traffic control mechanism? It's a roundabout and it's because

traffic flows. When there are collisions, because the movement is slower and stuff like that, the mortality rates are less, the damage to cars is less. It's more fuel efficient because people are not just sitting there idling. What causes a roundabout to be more effective and efficient as a control? People are risk aware; when you force them into the roundabout, they get nervous and they start slowing and looking more. With a streetlight or a stop sign, you know, they'll run them, they'll forget, they'll speed up, you know, all those behavioral things that actually create a more significant issue when an event occurs.

[00:13:04] And so I think in many ways, we have to take those concepts of my roundabout theory … There is in Chicago, I can't remember the street, it goes along the Great Lakes and there's a big bend in it. The transportation economist had started looking at it and the traffic control folks. People were always crashing because they were going too fast going into the curve, and it was a big, long curve. And so, what they did was they created stripes on the road and then shrank the width between the stripes to create the perception of speed. When people felt like they were going too fast, they took their foot off the gas.

"How do we present information to them, so their minds are open?"

Ashwin Krishnan: [00:13:43] Wow, OK!

Malcolm Harkins: [00:13:46] How do we do the equivalent of that with our users and our decision makers? How do we present information to them, so their minds are open and they make a better decision?

Ashwin Krishnan: [00:14:02] You have a great analogy, and I'll remember the roundabout. It's very, very true. That's how I learned while driving in India, though I had trouble coming out of the roundabout once I've entered it!

Malcolm Harkins: [00:14:11] Driving in India, though, it's like the mixture between Tetris and that thing with the frog, right? Having been in India a few times, even where there's lanes, there's no lanes!

Ashwin Krishnan: [00:14:25] [Laughs] So, coming back to something you mentioned earlier about your job title, which I found really striking, the Office of Social Responsibility. A particular incident that caught my mind was the CloudFlare outage, which I think was the first week of July. The thing that happened was less about the outage but more about how CloudFlare approached it. I was reading a blog by their CTO, John Graham-Cumming. It was, I think, about 13 or 14 pages long on exactly how a process ended up chewing up a lot of CPU cycles and that caused the WAF to go down, and so on and so forth. But the thing that I found most interesting — actually I posted about this on LinkedIn as well because I found it to be so striking — was their CEO, Matthew Prince, quoting his CTO's blog and saying, "Hey, this is how we screwed up." I took a pause and thought, you know what, this is not how security vendors usually talk about their failures. You mentioned Imperva, which recently had a huge outage, and we've obviously seen other major companies go to hell and back a few times as well.

[00:15:36] So given your role right now and your view of security vendors — because shit is going to happen, right, and you're going to be caught, and how you react to that really determines who you are and what you stand for — is that changing in the universe? I don't know how many security companies there are out there, maybe 6,000, 7,000, 8,000, whatever number there is, is there a percentage that are actually standing up and saying, let's have an office of social responsibility that roots ourselves in doing the right thing? We are going to be questioned, and when that questioning happens, let's make sure that we have all the controls in place to ensure we are approaching it the right way.

Malcolm Harkins: [00:16:25] Yeah, I think it is for some companies, and certainly in the CloudFlare case, that's true. I think my time when I was back at Cylance, when it was Cylance, that was true. I think what I'm trying to do at Cymatic is part of that. That's why it's a part of the security and trust office, you know, and trust is a function of two things: competence and character. Sometimes the competencies are the result of the capabilities, and sometimes we make mistakes. But the other aspect, there's a 50% part of that equation that is your character, your intent, your integrity. Are you deflecting things or are you blaming it on different things? Or are you covering it in a bunch of legality versus saying, we made a mistake; here's how we made the mistake; here's what we're going to do to fix and mitigate it? I much prefer that view.

> **"Trust is a function of two things: competence and character."**

[00:17:23] At Cymatic, I've drafted our privacy principles. I've drafted our corporate social responsibility principles. I'm starting to work on the InfoSec policies and stuff like that. But technology has an ethical and social responsibility for what it's doing and how it's doing it. And I think the security industry itself has a bigger one because it's there and its intent should be to protect its customers and society. And many security vendors honestly don't give a shit about doing that. They care about making money off of the pain of their customers. And many of them come with no shoes, and they have no social responsibility and no moral compass. And I know because I've interacted with many of them. Yet, I know the CEOs of many of them, a lot of them that I completely trust, and there are some that I don't trust because of the intent and integrity of the individuals.

Ashwin Krishnan: [00:18:29] Yeah, that's a great comment: Trust is character and competency. So any last words? I know we've covered a lot of ground over here on the people element. And I know you've talked a little about the future, whether it's utopian or dystopian, I don't know, whether you have the better chips than you have human eyes. Maybe I'm drawing a false analogy, but I'll try it anyway: the whole concept of bias and AI is if your dataset is flawed, your algorithmic predictions and your way forward is also going to be flawed. Are we at a point right now where we're setting ourselves aggressively for the future, but unless we admit our own failures and more importantly, make changes right now, this is going to be kind of rooted in our system?

Malcolm Harkins: [00:19:19] Yes. We will perpetuate and exacerbate the accelerated trends that we've already seen, if we don't hold ourselves more accountable, if we're not more transparent, and then offer up those learnings to not only the internal folks who need to learn, but to everybody else who may have felt the mistake that occurred. You know, there's a philosopher — again, another quote — Bergsten, who said, "Think like a man of action. Act like a man of thought." We've got to be action oriented. The actions that we take have to be thoughtful, not only for our companies and our organizations and our employees, but also more broadly, for society, considering the societal dependence we have on technology.

"We will perpetuate and exacerbate the accelerated trends that we've already seen."

Ashwin Krishnan: [00:20:11] Great comment. Malcolm, again, we're going to be doing this monthly, and I'm looking forward to future discussions. Thank you for your time and good luck in your new venture.

Malcolm Harkins: [00:20:22] Awesome. Thanks, Ashwin.

Ashwin Krishnan: [00:20:24] Thanks so much.