RSAC PODCAST TRANSCRIPT

OUR OWN WORST ENEMY: TACKLING THE SOCIAL ENGINEERING PROBLEM

December 7, 2018

As it turns out, the weakest link in any cybersecurity solution is...us. More than ever, hackers are using a variety of social engineering scams designed to fool people into giving up personal information voluntarily. So how do you protect us from ourselves? Hosts Britta Glade and Hugh Thompson and their guests Ira Winkler of Secure Mentem and Lance Hayden of Elligo Health Research have a wide-ranging discussion on what to do about the human problem, including establishing protocols, creating a Human Security Officer position and more.

Guests:

Ira Winkler
President
Secure Mentem

Lance Hayden
Chief Privacy and Security Officer
Elligo Health Research

Hosts:

Britta Glade
Director, Content and Curation
RSA Conference

Dr Hugh Thompson
Program Committee Chair
RSA Conference

Host: You're listening to the RSA Conference podcast, Where the World Talks Security.

Britta Glade: Hi, everyone. Welcome to the RSA Conference podcast. This is Britta Glade, Director of Content and Curation for RSA Conference and I'm happy to be joined by Hugh Thompson, Program Committee Chair for RSA Conference. Hello Hugh.

Hugh Thompson: And hello Britta and hello listeners. As 2018 draws to a close, we've been reflecting on the key trends and inflection points that we as an industry have been going through. The human element has always been a very important part of the security discussion but I think this year, in 2018, we really pushed the forefront and were able to see some of the biggest dangers of this human element take shape, especially in the form of social engineering. Is the new norm in hacking social engineering and will 2019 bring even more human-laced attacks? Today we're joined by two of our most popular RSA Conference presenters on a human topic, Ira Winkler and Lance Hayden. Gentlemen, welcome and please introduce yourselves to our listeners.

Ira Winkler: This is Ira Winkler, I'm president of Secure Mentem, which focuses on the human aspects of security and other things and also author of my latest book, Advanced Persistent Security, which is awesome. Anyway, I'll leave it at that.

Hugh Thompson: [chuckle] I like the book review. That is great. Okay and we're also joined by Lance Hayden. Lance, can you give a few words about yourself to our audience?

Lance Hayden: Sure, thanks. My name's Lance Hayden. I've been in security for about 30 years. I've had a lot of different roles. I've been a CISO, I've been a consultant and way back in the early days, I was even an intelligence officer, which is what first got me interested in the human angle of security to begin with and so I've studied and researched that for many years and written a book called People-Centric Security which tries to go in a more empirical model, how we can get it at human security and culture, in protecting our infrastructures.

Britta Glade: That's great, thank you both for being here and it sounds like we've got some good reading lists for people over winter holidays that are coming up. So take a look at the books that we'll have linked in here. Ira, I'm going to start with you for a question. I know you have some pretty strong opinions about social engineering.

In a nutshell, you've said, "It's not about training people to watch out for bad actors, 'Here's how they behave,' but rather, 'This is how you should do things correctly.'" So let's start this conversation with the stake in the ground. Why is this differentiation important?

Ira Winkler: Well, here's the thing, I used... If anybody saw my presentation last year with Tracy Celaya, I came up with the analogy of creating, essentially, Elmer Fudd or creating grandma's house. Most security programs regarding security... Well, social engineering, are basically creating Elmer Fudd saying, "Always be on the look out for the wascally wabbit." And everybody is there saying, "Oh, hackers are going to try to trick you, they're going to try to do this, they're going to try to do that." And I saw one security awareness company focusing on, "We make people afraid to check their emails." I'm like, "No, that's absolutely wrong. The job of security is to get people to do their jobs securely and be confident in how they do that."

So, anyway, going down to what I mean by grandma's house. When you go to grandma's house, let's say you go there with your parents for a big family dinner. You go there, your parents tell you, "When your grandma opens up the door, you're going to go in, you're going to hug grandma and kiss her." You're going to be like, "No, she smells." It's like, "I don't care. You're going to hug and kiss your grandma inside the door 'cause she's superstitious and then you're going to go ahead and you're going to sit where you're, only place left to sit 'cause everybody else knows where to sit and everybody does the right thing."

Now, going on to how this impacts security and why people should be doing things right in the first place. We're going to come up on W2 season and W2 floods really quickly now and right now, the way traditional social engineering security awareness is done, you're going to be training HR people to basically say, "Hey, there are going to be people trying to pretend to be somebody and trying to get you to mail out HR information. We don't want you to do that, be on the look out." And they would be like, "Well, geez, I'll pretend to be the CEO." But what happens if somebody emails you pretending to be somebody else? They'll be like "Oh, is this the wascally wabbit?"

The way it should be done is if you're a low-level analyst or HR analyst and you get an email, you should know what is the process for distributing information and it should be, there's an established process for releasing PII related information and they'll be like, "Okay, if I'm going to send PII information out, it's going to be encrypted to a known source and the IT department is going to be able to enable the encryption. Number two, in the first place, the request

should come directly from my manager. The manager is only allowed to authorize that if it comes from the CFO or general counsel or whoever."

Ira Winkler: And so if you have an HR person there, that HR person shouldn't be saying, "Is this the wascally wabbit trying to trick me?" That HR person should be saying, "Well, even if it is from the CEO, the CEO should have contacted my manager first, who should have the approval of so-and-so, the CFO." And so the process should be "Hey, I'm not going to decide if this is the wascally wabbit or not. I'm going to go to my manager and say, "Hey, manager, did you authorize this? Do you know anything about it?" The manager is going to be like, "No, I should check with the CFO."

Can some social engineer possibly go through all that? Yeah, maybe somebody's going to be a really good trickster but odds are they're not that sophisticated and if they are that sophisticated, you have a lot more to worry about. So, again, you shouldn't have a low level person on the front lines of organized crime, sociopaths and everything. There should be an established process to do things right, so that that low level person doesn't have the discretion to do it wrong. Sorry, that's my rant for the morning. I'll let somebody else...

Hugh Thompson: No, man, I like the rant. It's always good to start with a rant and Lance, let me bring you into this. Listening to Ira's self-described "rant" I think there's a lot of wisdom in there, a lot of folks that are trying to do their jobs, often when they're put under time pressure or when social engineers use some of the tricks of the trade, like pretending to come from their boss and using authority and trying to get them to do things that maybe they normally wouldn't do. I'm just curious, how do you think the practice of social engineering, as applied by the attacker, has changed over the last few years? Do you feel that it's changed and is this threat getting worse or better or is it the same as it's always been?

Lance Hayden: Yeah, so I look at this, I started out my career 30 years ago as, again, like I said, a human intelligence officer and so for me, I never think social engineering is something that's new, it's actually for me the oldest attack in the book, we've been doing it forever and it's about someone realizing that they can take advantage of another person's naiveté or vulnerabilities, personality or just their innate trust, gullibility, whatever you want to call it but it's an inherently human problem and it pre-exists technology by a long, long time.

And so I don't think that it's anything particularly new, I think one of the reasons that it's becoming so prevalent and so common and dangerous today is, at the end of the day, the way that I like to treat it is, this is an infrastructure problem and what's happening is, attackers are realizing that some of the infrastructures that they traditionally tried to go at around technology and other areas, that the attack surfaces of those have been fairly locked down but there's a very ripe attack surface around the human infrastructure that security, to it's discredit, has not paid very much attention to over the years.

For as long as I've been in security, we've talked about security as a people, process and technology problem and those are describing the three primary infrastructures within any kind of organizational security program, within any, really, organization in general and what I like to use, the analogy I like to use is, it's like that... We do security, we're like that guy at the gym and everybody has run into this person at the gym and it's this individual that is always in the gym but they're always doing upper body work and so they've got this enormous torso, they can bench press a small car but they don't ever do leg day and so they've got skinny little legs and they never get on a treadmill so their cardio... If you put them on one for five minutes, they pass out.

And so it's this sort of over-weighted portfolio and when you bring that into the security, the reason we're like that guy is because when we start talking about people, process and technology, we mostly focus on technology. So we're, again, we're like that guy. We've got this enormous technology torso that's really buff and strong but we've got these skinny little process legs that we're standing on, 'cause we don't pay nearly as much attention to that and people are like cardio.

Human beings don't have a command line interface so therefore they're inscrutable so therefore the best way to handle that infrastructure is to try and automate it out of existence and again, you can throw tons of different analogies of that but if you have again, a three-legged stool and two of the legs aren't as long as the other one, that's not going to be a very stable piece of furniture and it doesn't work when you're talking about furniture and it doesn't work when you're talking about security programs.

And so the reason that social engineering is this big bugbear right now, despite being probably the oldest attack, in my opinion, is simply because that is the least analyzed and the least addressed security infrastructure that we have and we have neglected it for a long time and

hackers and attackers aren't dumb and eventually they get wise to, "Oh, this is where the most vulnerable attack surface is, this is where I'm going to go with my attacks" and it's as simple as that.

Ira Winkler: Yeah, can I add to what Lance said or do you have a question? Sorry.

Hugh Thompson: No, no. Go for it Ira.

Ira Winkler: Okay. So I think Lance's people, process, technology, I agree with. However, one thing that's critical is there needs to be coordination. There's a difference between being a stool and trying to balance yourself on three poles and the problem when you're dealing with the human issue, using that analogy, is that most people are balancing on three poles, not having a stool to bring it together. That's my latest article on human security officers. Somebody to bring that together because yeah, somebody's going ahead and somebody is saying, "Okay, we should have anti-virus software, we should buy anti-spam software." and then somebody's out there putting together an awareness program and I'll come back to that in a second and then somebody else is out there saying, "Well, we have these policies, procedures and guidelines and we're going to have that." But nobody is there saying, like in my previous analogy, "Okay, somebody is going to attack a human asking for PII, what is the process for that, bringing it all together?"

And just using my example, the process should be, in the first place, if somebody sends an email saying I'm the CEO, a spam filter or something should potentially filter that out or isolate that message. Then okay, the user has processes, procedures and guidelines that are coordinated and say, "Okay, we understand somebody's going to try to trick somebody, not what is a policy we show to auditors once a year." And how from a human's perspective do we implement procedures that say step by step how to make sure this doesn't happen and then the user has to be made aware of what those processes are and then, from that point, there's also some technology like data-leak prevention software that stops it from getting out, if the user falls for it.

So again, we need the process, people and technology but it has to be coordinated. Now, along with that, the other part is the problem of making people aware of social engineering. There's this kind of... I hated this, I've been known for saying, "You can train a monkey to hack a computer in a few hours" which to a certain extent is true. Because really, here's the problem; breaking into something is completely different than stopping it and, in our world, we have people say, "Oh, well that guy knows how to break into a computer, let's make him fix it as his punishment." Just 'cause you can break a light bulb doesn't mean you could put the light bulb together or invent the light bulb in the first place.

Likewise with people, I hear everybody saying, "Okay, well a hacker's going to try to tricky you, tell people not to fall for that trick." It's much in the same way, you can't just make it that simple because that's another part of what Lance was alluding to. You can't just make it simple and say, "Well, let's just tell people not to fall for these tricks, which is currently the state. I hate to call it the state of the art, it's the state of the lack of the art and awareness because right now, we're training people and we're giving people squishy toys and trying to get people to remember things.

We need to have an awareness program that really creates the culture and that's another aspect, we need to create a culture. I worked at NSA, Lance worked at CIA, if you don't wear your badge when you're inside the building, you get stopped. Believe me, you're going to wear a badge. We go ahead and if we're sitting there and say, "Oh, I'm sorry, I left this top secret document in my pocket as I walked out" hell, you might get arrested first before they investigate. The state of the art and what we're doing to prevent or educate people about social engineering is rather poor. I'll leave it at that for now. Sorry, I ranted again.

Britta Glade: No, no, I love all the analogy slang. I can tell you both are so focused on the human awareness and how our brains remember things and process. There's been many, many analogy slang here. So Lance, I'm going to circle back to you from the self-proclaimed first Ira rant. What do you think is most effective? And backing this up with, our human element track at RSA Conference has exploded over the past few years, both in terms of people who are showing up to attend the sessions, as well as the number of sessions that are being submitted of people wanting to speak in that track and there is a growing divide with how do we best teach employees? Do we reward? Do we shame? I suppose we could draw these same parallels into parenting being done and different things people are putting out there to how do I teach my child about bullying? What's most effective? How do we really, really, really move the needle on changing how employees behave.

Lance Hayden: Well, that's a really good question and I'm going to loop back and tie it into what Ira was saying earlier too 'cause I'm in violent agreement with him with the

difference between the stool analogy and trying to balance on three poles, we have to bring these things together and often, they're done in siloed ways and as separate kinds of activities and even worse than that, they're often done in silos that have more or less antipathy towards one another. Nothing makes me madder than hearing one group... The whole concept of, you can't patch stupid. I hear that all the time and stupid is always what someone else is doing, it's never the mistakes you made, it's always the mistake someone else made. So everybody thinks everybody's stupid and then this has really lend itself to effective security culture.

And so I think that one of the areas is, is it reward, is it punish. I tend to go a third route and say it's include and one of the areas where I think is it's seen as cutting edge, where you're really seeing this kind of bringing things together is in the DevOps and more specifically the DevSecOps space where coming out of development teams and agile software mechanisms, we're realizing that we have to pull these disparate groups together and in DevOps, it was that idea of bridging the gap between development and operations and making them work together and then the natural progression of that is moving security into that too.

But the way that that works is, you have to create a tightly coupled system, where security isn't an afterthought and isn't an outsider that is brought in to advise or comment on what the other teams are doing. This is a tightly coupled unit that has elements of all three in the context of software development and software deployment in modern software architectures and so that's one where they really get it, that they're all bringing critical functionality, whether that's functional or non-functional requirements, those requirements are being met by these teams in a very specific way. I think trying to push that out to the rest of the organization in areas that aren't necessarily development operations but just business operations, we still have a long way to go on that but that's probably a very fruitful angle, I see a lot of potential there.

The other thing, it's interesting. Ira, I read your article on the case for the human security officer in Dark Reading and it really struck me, going back, we talked about both of our mutual experiences in the intelligence community and as I was reading it, I'm like, Ira's describing essentially a counter-intelligence chief. Again, looping back to this not being a new problem, when I was an intelligence officer, we had a specific role in a specific group within the intelligence agency that was inward looking, it was designed not just to Ira's point, to point out and slap people on the wrist for bad behaviors. This was someone that was responsible for understanding the human vulnerabilities and the human security posture, within that organization, in a way that would prevent secrets from being lost, whether those secrets were inadvertently lost or whether they were lost because someone tried to penetrate the intelligence agency.

And so I see echoes in that as I was reading Ira's article but that's what this role needs to be and I think the irony of that is if you go back and you look at... I just finished this great book, I like spy books and so Ben Macintyre released this book The Spy and the Traitor, about Oleg Gordievsky, who was a major KGB defector to MI6, talked about this and the problem was that Gordievsky was given up by another traitor named Alder James and Ames was ironically the chief of counter-intelligence for Soviet Intelligence inside the CIA and so even way back then when this happened, the problem is that counter-intelligence just like sort of security awareness today wasn't really considered the cool job within intelligence or as security awareness still, even though we are getting more traction on the human security side, it's still not considered as cool as being an offensive hacker and again, that was something else Ira talked about.

I think that what we need to do is really humanize security and make it clear that if you have an organization and you go to that organization tonight and you throw all your technology out the window, when everybody shows up for work tomorrow morning, you're still going to have an organization. Because at the end of the day, an organization is made up of people working towards a common purpose. If you go to your organization at night and you fire everybody, what's going to happen tomorrow is you're not going to have an organization, you're going to have blinky lights and wires and whirring fans that's basically just a warehouse of gear that doesn't really have a purpose anymore because without the people, it isn't an organization.

And if we're going to improve organization security, we're going to improve enterprise security, then we have got to get it into our heads that the first line of defense is the people that make up that enterprise and addressing those human problems and to Ira's point, not turning this into an adversarial relationship but turning it into a collaborative one, is going to be absolutely critical and again, we've known this for years and years and years. It's the only way to fight the problem.

Ira Winkler: Yeah. And just let me add...

Hugh Thompson: Yeah, go ahead, Ira.

Ira Winkler: Because I have another way of looking at it. You're saying, is it the carrot or the stick? It shouldn't necessarily be either because here's the thing, when somebody comes in, do you tell a new employee, it's like, "Well, we'd really like you to fill out a time card because we need to track it and it's really important for our processes and so please fill out the time cards." It's like, they fill out the time card 'cause they don't get paid if they don't fill out the time card. It's not a punishment, it's not a carrot, it's basically, this is part of your job function. At what point... I was on a panel, a keynote panel for ISAC a few weeks ago and I was sitting there with a bunch of CSOs and they were saying, "Oh, well, we can't blame the user," I'm like, "Why isn't security a fundamental expectation of their job? Why does it seem like we have to encourage them to do what should be a critical part of their job and that's something that has baffled me.

Like an accountant, you don't hire an accountant and say, "Look, you're an accountant, you're supposed to track our money and make sure everything's okay. Well, here's our accounting software and generally use this. Oh and people are going to try to steal it, try to do it right and find those people." You don't do that. You basically hire a new accountant, you say, "Here's the software, here's basically how you do your job, here's how you categorize everything. You do your job A, B, C, D, exactly like this, like everybody else has been doing it and if there's any discrepancies, let us know, 'cause then we will investigate." Why isn't security checking things? Wearing a badge, making sure people don't follow you in, just a fundamental expectation of this is how you do your job right, as part of doing it right. Like every other aspect of their job. I'll leave it at that for now.

Lance Hayden: I think that there's... I think that Ira's got a point there but I also think that there's a counterpoint to be made and that's that there's cultural conflicts that happen that influence this and so the idea of, Ira you mentioned tailgating and the idea of, "Hey, why isn't it just an expectation that you would check people's badges as part of just... That's just a fundamental expectation of your job." And I can totally see that. I think though that what we often do is we often give people inside organizations competing cultural priorities and so in the case of tailgating, what I've seen, in my experience, is that the two cultural traits that come into direct conflict there are the security culture, which is, "Trust no one, verify everything." and the more trust and... How many organizations like to think of them, "We're not a company, we're a family, we all trust each other, we're all in this together."

And when you put those two things together, what you end up with is, if you're coming in the door and you see someone coming in carrying a heavy package and struggling to get the door open, you immediately get this sort of cognitive dissonance, "Oh, do I stop this person and say, 'Hey, before you even open that door, I need to see your badge, put down your package.'" Or, you're like, "Oh, this is a colleague and someone that I work with, I'm going to open the door for them and help them 'cause they're obviously struggling to get this package in the door and those are some that are happening on an unconscious level and the fact of the matter is, as human beings, most of us and Ira, I'm not sure this applies to you, [chuckle] but most of us prefer to be trusting first and skeptical and suspicious after. It feels better to trust.

Ira Winkler: Okay, let me interrupt you lightly and then... I will just make this point. I am not saying that... What I'm saying is, we are here identifying, for lack of a better term, an ideal and a principle. The fundamental principle is and I use tailgating as examples where there's expectations of doing things right. I appreciate what you're saying that we have to change it, the problem though I see with security as in handling the human and I'll address it this way in summary, is that the problem is, we have people who are afraid to address the culture of the organization as a whole, that they think, "We don't want to impact anybody, we want to be friendly and we're not going to set up any strong expectations so we're just going to try to make people more aware" and I said more aware. Oh, yeah, they will do it because they'll know it's the right thing to do, that doesn't work.

Here's the thing, security is not about perfection. Security will never be perfect and yes, there will always be people who will allow a tailgater through. The issue though is, do we allow cultures and because everybody says we want to create a culture, you have to define a culture. It's kind of like, if I take my kid to a buffet and I can sit there and tell my kids, "Okay, you should have fruits and vegetables and primarily," sorry, Lance is a vegetarian. It would be sickening to go to a buffet with Lance. But anyway, if you have all these... If you tell your kids everything and you should have fruit and vegetables, they will go to the buffet, you'll leave them on their own, they will go to the buffet, they will come back with a grape and say, "Look, I got a fruit, didn't I do good?" And that grape is on top of every type

of chocolate cake and ice cream and everything else that they could've got because that's what happens when you let people to define their own culture, even if you educate them.

Ira Winkler: So it's not about, yes, there will be some sort of angst and competition between people wanting to be human and people wanting to be secure but the problem is we've advocated, or I should say security programs in general have advocated their power or authority to the whims of average users and I'm not saying there's one or the other but I'm saying they've kind of totally given up and said, "We'll just encourage people to do things right" and that's just so wrong.

Lance Hayden: And I think that Ira makes a really good point about security. I think that security is not about fear, it's not about carrot, sticks, all that. It's really about habit and creating these habits and the analogy of the buffet and trying to get your kids to eat right, I think another way of looking at it is to say, let's say we go to that same buffet and I tell my kids yeah, you should be eating fruits and vegetables and all this healthy stuff and then I go to the buffet and I come back with the meat loaf and the corn bread stuffing and the chocolate pie and the one grape.

My kids aren't stupid. They're going to look at that and they're going to be like, "Okay, yeah, do what I say, not what I do." And I think there's a lot of that going on too. It's one thing to talk about, everybody in the organization should understand security as a good business practice and do the right thing but let's face it, there's a lot of times when the clichés are, we'll go in and that only applies to users, it doesn't apply to senior management, it may not even apply to security team. I've been in situations where the security team can be fairly dictatorial and arrogant about how they look at the rest of the organization.

It's hard to go in and tell someone out of one side of your mouth, "You're a very important part of this and you really need to understand how to do things right" and out the other side of your mouth be like, "But you're not really smart enough on these issues to really make any informed decisions, so you should defer to me on everything." And I think that again, culture is a complex beast and it has a lot of different competing priorities and most of those priorities, to make it even harder, are not even competing at the level of conscious thought. Culture is not something people go into an organization and recognize on a day-to-day basis, "Oh, this is my culture. Oh, I'm doing something cultural right now." It's something that's transparent, it fades into the background, it's just... One of the best definitions of it is, "Culture is just the way we do things around here."

And so that gets ingrained as habit and I agree with Ira. Ira, I agree with you, I think that one of the things that we have to do is figure out how we change habits and whether or not the current state of the art on awareness campaigns is effective and the squishies and the gamification and everything else. I tend to have my own sort of skepticism on some of that as well but what I do think it is, is I think it's an attempt to try and find a different avenue to get at this problem and to really start trying to make micro changes in people's habits and perceptions that could potentially lead to that state that you're talking about, where we want to get to people where it's much more of an innate ability. But I completely agree that we're nowhere near that yet and that we've got a long way to go.

Ira Winkler: Well, the thing is, and I'll just use this as an example, you and I... I use the badge as an example, that means like working at NSA, there was one time I was on shift work in NSA and when I had to use one of these graphical plotters, I had to take my badge off and everybody wore their badge in NSA and you had to and there was one time I was working late at night, used this plotter, left my badge on the desk and went to the bathroom accidentally leaving it on the desk and as I was out in the hallway, there was a guard saying, "Where is your badge?" And I was like, "Okay, it's probably at my desk." And then the guard's like, "Okay, we're going to your desk." I'm like, "You're not allowed anywhere near my desk," he's like, "I'll wait by the door." So the guard waited by the door and then I go looking for my badge and I'm like, looking around the desk and then after... As the guys see me he's like, "Are you looking for something, Ira?" And it's one of my co-workers. I'm like, "Where is my damn badge?" And I was obviously cursing at him and the guy's like, "Do you mean the badge that should be around your neck?" And then I'm like, "Give me my damn badge." And the guard's like, "Is there a problem here?"

Do you think I ever forgot that badge again? And the reason was it was innate in the culture that was created from management down that caught me because culture... When somebody asks me what is culture and what's awareness, if you have a good culture, you don't need an awareness program because everybody starts doing what everybody else is doing and frankly, even if you have an awareness program, it's irrelevant. Everybody's going to do what everybody does and so you have to impact what everybody does if you want to have a good culture

because, at the end of the day, awareness and social engineering prevention is essentially an outgrowth of the overall culture and organizational procedures. I guess I should ask Lance, did we have moderators on this call or anything?

[chuckle]

Hugh Thompson: We're here, we're here.

Britta Glade: We're eating the popcorn and just listening along. It's been a great conversation.

Lance Hayden: Yeah. And on that note, I'm going to dive right in there before the moderators get a chance to talk too because I think... I agree with you, again, I think that culture is also more than just shared habits and it's more than just behavioral. I have my own sort of security story from the old days and same kind of thing, I screwed up during a security... We locked everything down at night and I didn't lock something down correctly and so I got written up for it and even more than the sting of getting written up for a security violation, what really bugged me was this sort of deep-seated fear that it was a sensitive business and I had let my colleagues down. I could have potentially... If something had... If that had been a really bad security incident and it hasn't just been on me of not locking a safe or something. If I had actually caused some sort of sensitive information to get out, that could've compromised someone's operation. It could have potentially caused a loss of life and so it wasn't the slap on the wrist that really bothered me, it was this idea that I had let down the other people in the organization and that if all of us didn't take this seriously and professionally, then we weren't going to have an effective intelligence organization.

And so I think that in addition to the behavioral side, it's also... It's not just shared habits and behavior, it's shared values and that's one of the other things that has to be instilled in the entire workforce, is this idea that security is important because if we have a security incident, then someone is harmed by that incident and not just me, 'cause I got fired or gotten written up, I've let someone's medical records get out into the dark web. I've let someone's financial records get exposed, whatever, I have caused harm to somebody and I've let down my colleagues and I've let down my customers and it is values and sort of prioritization of what really the company is about. As much as it is, "Oh, I don't have the right habits or I don't have the right behaviors" in this particular situation.

Ira Winkler: Yeah, to go to what Lance is saying, that goes to again, three good concepts of what an awareness program is comprised of; there is, at a high-level, awareness of what the problem is. Then awareness of what the solution is but most important, the motivation to implement the solution and Lance described the ideal form of what he considered motivation for that. Now I'll shut up there.

Britta Glade: No, I was actually going to ask you guys, for the wrapping points and what's nice is the closing arguments have been made by both of you. I have furiously been taking notes here. Interesting things. Human being is a complicated creature but I think you've given our listeners all kinds of ideas in and around culture and habit and modeling and inclusion. I love Lance's parallels to DevOps. I'm intrigued by how that has developed and what's going on. There's some really interesting things going on operationally and otherwise in the world of DevOps, which is also reflected at RSA Conference.

But this has been a great conversation. A lot of actionable things, a lot of introspections that I think you'll allow for listeners. So thank you both for joining us, thank you Hugh for being here on the couch with me eating the popcorn and just listening to the back and forth. This has been a really great conversation.

Hugh Thompson: Oh, this is great, thanks. Thanks for joining. Thanks everybody and we'll see you on the next podcast.

The mission of RSA Conference is to help professionals stay on top of cybersecurity trends, issues and solutions through our global events and online content. Visit rsaconference.com today to read posts from industry leaders, view Conference session videos and presentation slides, see more special reports like this one, and receive exclusive offers on upcoming conferences.

Visit RSAConference.com

Follow us on: #RSAC