**RedZone Podcast Episode #53: Security Begins at the Heart and Not the Head – with John Sileo**

\*\*\*  
Bill: What was it like trying to interact with your kids going through that?

John: Yeah. It was all consuming. You're right. You're already busy enough doing your job. Then you add this incredibly invasive, live changing event like a court case or being convicted of something you didn't do. It took almost everything from me, almost including my family. There's a time when my oldest daughter, who was five when I was going through this, came down into my little basement office. You got to understand, I'd spend my nights, my weekends, my free time, trying to a) resurrect everything that my choices had brought. They were my choices. He was the business partner I brought on, I didn't vet him. I didn't have user level permissions. I let AR and AP be controlled by the same ... Anyway, my stuff and I'm down there trying to just pay the mortgage and stay out of jail. My oldest daughter comes padding down in her pajamas with her little stuffed dog and a book and tells me it's story time. I'm so ensconced in just trying to keep myself out of jail that I kind of push her off and I tell her, "Hey, what I'm working on is so, so important." She looked back up at me with her little stuffed dog and the book in her hands and she's five years old and wearing pajamas and says, "When you're done, dad, can I be so, so important?"

That's just the point at which I finally cared about this stuff and people shouldn't have to go that far into the rabbit hole before they start to pay attention for their selves, their own personal identities, and by extension, for their businesses.  
\*\*\*

Bill: Let's get started. I want to welcome you to the show today.

John: It's so good to be here, thanks for having me.

Bill: Yes, I know. It's taken us awhile to get together and I'm super excited we're able to connect. We've got to start this out with you story. Your book Privacy Means Profit, super, really wonderful book. We're going to talk about more of the book as we go along, but you've got to share with listener's this story of how this all began. You're this front end leader right now of this movement in privacy. Where did this all begin?

John: [00:01:00] I kind of got started by making all the mistakes really early on that we now see all the way up through the corporation and government. Ten, twelve years ago, I had a case of personal ID theft where a crime ring called the Cash Men stole my identity out of my garbage after buying a new home. Back then you throw away copies of documents, don't even think about it. A woman purchased my stolen identity and used it to buy a home and commit some crimes in my name and drain my accounts. It basically kind of a garden variety dumpster diving type incident. After that, I took kind of the basic steps we all do, got a shredder, froze my credit, did a couple of things. I never made the jump to my business.

[00:02:00] I had started a software business with my rock climbing partner, my very good friend, Doug. It was a spin off of a family business that I had taken over after being in management consulting. It turns out that Doug, this close friend, rock climbing partner, person holding my life sixty feet in the air, used my identity to embezzle from all of our clients, close to a half a million dollars from our clients. It looked like me, but it was him. I then spent the following two years in a criminal trial being the lead suspect. Pretty much destroyed everything, destroyed our, here it was a forty year old family business in Denver. It destroyed the reputation of that business. Destroyed the actual business, lost three hundred, four hundred thousand dollars because we paid back the clients who had been harmed. Doug, my partner, never paid so much as a penny. He declared bankruptcy.

[00:03:00] In that, I realized all of these things, this connection between our personal security and our workplace, our business security. This phenomenon that it's all selfish, security's selfish, it's not a department, it's not a job description, it's kind of this emotion of how you protect what's important to you. For me, I lost two years with my family. I lost hundreds of thousands of dollars. I lost my business. I lost kind of everything. That has given me a really neat platform from which to share with people because I am the one who's vulnerable. I am the one who's made the mistakes, who can kind of share this outward and say, "Listen, don't do what I did. Think about this before it's too late." It's given me this amazing career speaking around the world to conferences, especially when I need to light the fire under a technical crowd or under a leadership crowd who doesn't quite see, "Hey, this isn't just about me. This is about my job. This is about our company. This is about societal goodness."

Bill: [00:05:00] Yeah. I don't think, we talked about this from your story. I went on your site. I listened to your, I think it was a 60-Minutes clip or something. You talking about the story in more detail. It made me go back to when I got sued. I had over eight hundred thousand dollars stolen from my organization and I don't think people generally understand the impact that fighting a lawsuit has on one's life. I mean you're out there trying to take care of customers, bringing in revenues, paying expenses, dealing with employees, all the normal, all the regular stuff that you expect an entrepreneur. Then you throw in lawsuits on top of that, or a lawsuit. When you were talking, the emotion that I, brought me back to trying to- What was it like trying to deal, work, interact with your kids going through that?

John: [00:06:00] Yeah. It was all consuming. You're right. You're already busy enough doing your job. Then you add this incredibly invasive, live changing event like a court case or being convicted of something you didn't do. It took almost everything from me, almost including my family. There's a time when my oldest daughter, who was five when I was going through this, came down into my little basement office. You got to understand, I'd spend my nights, my weekends, my free time, trying to a) resurrect everything that my choices had brought. They were my choices. He was the business partner I brought on, I didn't vet him. I didn't have user level permissions. I let AR and AP be controlled by the same ... Anyway, my stuff and I'm down there trying to just pay the mortgage and stay out of jail. My oldest daughter comes padding down in her pajamas with her little stuffed dog and a book and tells me it's story time. I'm so ensconced in just trying to keep myself out of jail that I kind of push her off and I tell her, "Hey, what I'm working on is so, so important." She looked back up at me with her little stuffed dog and the book in her hands and she's five years old and wearing pajamas and says, "When you're done, dad, can I be so, so important?"

That's just the point at which I finally cared about this stuff and people shouldn't have to go that far into the rabbit hole before they start to pay attention for their selves, their own personal identities, and by extension, for their businesses.

[00:07:00]  
Bill: Yeah, this is a dark, dark place you went to. I think, clearly, the gift from this is that you're passion for education and helping people not go through that same experience. It's no small point as well, not only the impact, but the ethics that you went out to try to repay these pieces and take personal responsibility. I mean, there's just so much positive wins that came out of this. Years ago, it wasn't a win in your basement, but now, just even a look at it from also like hero's journey that you went through.

John: [00:08:00] Yeah, it's been a journey. I can't say that I'd want to go through that again and have those several years of sleepless nights and fears of going to jail and of bankruptcy, you know, all the other stuff that comes with that. I'll tell you what, I consider myself one of the lucky ones that I get to go to these amazing places to speak to people and meet amazing people who, by the way, many of which, like yourself, Bill, have had an experience of some sort and, man, if we can tap into those personal experiences that CEOs and CISOs and everybody have had. That's where the real power comes from. That's a transformative connection between the personal and the professional.

Bill: [00:09:00] Yeah, and that's what I found really unique about your book and your message is that you take and you're very clear about this, taking this personal impact and making it and then linking it back to the business. At times, it can seem so antiseptic. "Oh, it's a big corporation. They just had theft." You really don't- Identity theft or just got hacked. It's just so, you become dull to it. You have this resonant story. It was that- How did you link the two together to make it unique for you?

John: I think it was so clear to me at some point that security starts in the heart. As I traveled around to these organizations that have breach or are preparing for breach to the targets and the anthems. These conferences that I speak at, I started to understand that they all thought that security started in the head. That it's somehow a policy or a procedure or an academic pursuit. For you and I, for the person handling the data every day, it's our connection to our kid's Facebook page or to how much information they're sharing with GeoTagging or letting people know that we're out of town because of something we post or how we protect our smartphone. That's where we actually care about this stuff.

[00:10:00] It's been ten years of a hundred presentations a year and meeting with the people afterwards to understand what they really care about is the personal. They're certainly willing to expand that into their workplace but don't start with the workplace because you're talking into deaf, deaf ears. Start with the why of security. For me, my daughter, letting me know, "Hey, dad, you're not here for me anymore." That's what we're protecting. That's what's at the end of the social security number, the credit card numbers, the breached database.

Bill: [00:11:00] I noticed, also in some of your talking, John, that you bring humor into this, but it's a very unique type of humor where, well maybe you can explain. I just noticed your audiences were actually kind of light, they were lighthearted while you covered this kind of serious topic. Again, was that something that you crafted intentionally, or is that just your style of making a point and not being so dreaded about it? Maybe share a little bit about that.

John: [00:12:00] I think there's kind of layers of the onion on this one. It's a serious topic, right? It's also kind of generally a dry topic, as you mentioned. To present it in the same old way, death by PowerPoint, doesn't work. I've done, in addition to doing years and years of research on these topics, on cyber security and data protection, I've also looked a lot at the deliver, the pedagogue of it. First and foremost, I'm a professional speaker. I'm there to wow the audience, to get them to take even one step to- The most important thing for me is that they walk out of the room doing one thing. If I can interact with them and make them laugh, rather than preach at them and stand on a soapbox about all of this, they remember it. They walk out. One of my signature moves is called the hogwash. I go out and I socially engineer the audience, two, three, four, five times, to show them how difficult it is when a professional is working on you for information. I tell you what, they walk out of that conference and they chuckle and they, "Hogwash" to each other throughout the rest of the conference. It just builds and builds and their brain chemistry changes. It's the humor that people connect with. They love that interactive aspect.

Bill: [00:13:00] That's great. My team, we're a bunch of security gearheads here. My CTO, of course, is the leader of the bunch. When he came back and started talking about I got to see you. I got to see you. I was like, "But it's not your typical speaker, James." He's like, "No, this guy is so good." It's interesting. It seems like you're transcending both the business audience and the deep technical audience as well, which is really where we really need to grab them both audiences, which is fantastic.

John: [00:14:00] Well, listen, most people in my audiences, in that type, that ISOC conference or another technical conference, honest to God, these people know more than I do. They're more versed in the topic than I do. What they don't have is the benefit of that kind of human element perspective. They don't have the benefit of seeing if you shift your thinking, God, even forty-five degrees, from what you have now, all of that knowledge you have built in and you apply it in a slightly different aspect, through the view of the human being, not through the view of a corporation, everything changes. The culture of the organization, the culture of security, the habits that people are willing to build, the behavioral changes that come on that, that is what makes a C change, and it makes it quickly. Companies and corporations and even the department of defense that I've done a ton work with, they see how powerful it is to have it be that method rather than just share information.

Bill: Let's talk about this culture of privacy, which again, I found very unique. Sometimes it can get so dry and boring and so non-transformational just reading checklists and tasks and to-dos and these lists of things that you need to protect against. What do you think is the most- Walk us through your idea about building a culture of privacy?

John: [00:15:00] It's kind of a, I think of it as a web, kind of a a web of culture. There's human aspects of it. There are physical aspects, physical security. There are technological aspects, the devices. There's kind of this network or internet aspect. Those four areas weave together. I always start with the humans. Frankly, in an organization that doesn't have a culture of security in any way, I start with the top. My very most important audience is the ten people on the board of directors or the leadership team or the entrepreneurial team, whoever it is, because they need to- If they don't understand, if they don't get that Sophie moment, that's my daughter's name, that moment where you lose it all and you have no idea what just happened to you. If they don't understand security, they don't fund security. You've got to have that buying in on the board.  
[00:17:00] Look at Target. Did they have a CISO on the board before the breach? No. Is that a major cultural red flag in terms of? Yes. If the board's not talking about where they are in terms of identifying their most valuable data and what they're doing to protect it, they're not a benchmark best in practice company yet. Getting that board buy in and then really it comes down to, you have to serve your people first. When I go around and Pfizer's a great example. Pfizer brought me to speak at every campus that they had because they understood that if you don't get those people one by one interested in this and you do that by starting with their security, by getting them interested in security period, whether it's corporate or personal and building that from the bottom up of, "Hey this stuff matters. By the way, it's your job. It's your responsibility." I soft shoe those type of recommendations because I don't want to be preachy. When they come out they know that their job depends on the way that they're protecting that data and building from the bottom down, trickling down or from the top down and the bottom up, culturally, that's really what changes things. Then from there, you kind of have to habituate people in the right ways.

Bill: [00:18:00] I'm so glad you brought this up, because one of the big reasons I go to some of the top security conferences is not that I or my company is working with Coke, Pepsi, Pfizer. These supposedly have the best of the best IT security professionals, fully staffed. I'm going to them because I want to hear what they're talking about to apply it to the small, the medium enterprise, the ten person to the ten thousand employee company, because what's interesting is we can't scale security devices. When you go into individuals, that's a much quicker return. If you go to the board and say, "I'm going to educate your people and it's going to make you thirty percent safer because they're educated." That you can scale knowledge into people fast, versus having to buy fifty-five security devices for seven million dollars.

John: Totally. I don't know if you've read, what was it, Power of Habit.

Bill: Oh, by Duhigg.

John: Duhigg. Duhigg, yeah.

Bill: Yeah, yeah.

John: [00:19:00] The story of how [Koa 00:18:20] and [Paulo Neo 00:18:20], who took over this failing company that was way below earnings and changed one factor, took one keystone habit, which was worker safety. He takes this one habit and it ripples out and it changes the level of quality that they're quality control. It changes the way that people feel about the job because they're not safer on the job. Here, several years later, they've got five hundred percent profitability of what they had before, because he looked at one really important habit. Guess, what, phishing is that habit or password protection can be that habit. If you do it right, you can have that spread like wildfire where you put it out to the managers and it builds from there. Guess what, if you learn phishing, you've learned the basics of social engineering. If you're learned social engineering, you don't pickup the USB drive in the parking lot. You don't let the person in with a handful of donuts at the back door after a smoke break. You don't take the phone call saying, "This is your IT department. We need to get into your computer." It's so pervasive once they get the basics, but God, you got to give them the basics.

Bill: [00:20:00] That is funny. I haven't read the whole book, Duhigg's book, but I have it staring at me in the mornings. I have read enough of the book to read that story. That story, so funny you picked it. That's a really powerful story, how one- It actually doesn't even follow a pattern you think a CEO would tackle, like worker's safety increase profits? They probably thought he was crazy. It sort of follows an interesting path, John, because you're right. If you educate people not to click things they shouldn't be clicking and why, you potentially eliminate ransomware or decrease the likelihood by massive percentage points, much more frequent than just having fancy toy that you buy. I say fancy toy. I don't want to belittle security technologies, but the fact is, people, to the point, it's a habit. If we habitually train people like you've done at Pfizer, then that has a ripple effect, which is so powerful.

John: [00:21:00] Yeah. I'm with you. You don't want to belittle the technology and the intrusion detection and the data loss prevention. That's all a part of it. I know the emotion that you're coming from, which is, there's so much focus on that that we forget the other. Yes, is that part of the web of security? Yes it is, but we're all kind of already taking care of that or have started taking care of that. What we haven't done is to train Fazio Mechanical to not allow access and to target servers and third party access and carelessness in the workplace and even vetting out maliciousness in the workplace, the inside mole job or those type of things. I'm so glad to hear you say we can't focus so much on the equipment and the technology that we forget who wields that technology.

Bill: [00:22:00] Exactly right. In your book you go through some statistics that I want to ask you about, but what's interesting is the human error. It's funny that they had to address human errors because people were dying in operating rooms not because of the surgery, because of the infections caused by human error. It was a massive problem, people dying. I think human error is the issue that which you're addressing is how do we fix human error by training and by educating and by making it personal. I think what a powerful platform that you're on right now.

John: Yeah. I'm really happy to be in this spot.

Bill: Let's talk about CIOs for a second. There a quote in here that said, "Of the CEOs, so the E, fifty-three percent said that the CIO's responsible for data protection, yet only twenty-four percent of C-levels would point to the CIO as the one responsible for data protection." I thought that was interesting. Then, "Of those who are said to be in charge of data protection, eighty-five percent wouldn't believe that a failure to stop a data breach would impact their job."

John: Wow.

Bill: [00:23:00] I was reading this in your book and I thought, "Well, that's true. I mean I believe that. I actually believe it." I guess it would start, you'd have to have the assumption that a CIO or CISO if they've broken that job off from the CIO, that could actually believe that they could stop a data breach.

John: [00:24:00] I want to share a provocative opinion here that is mine only, but I'd love to hear back. I don't know if you have a spot for your listeners to comment, but, to me security is not the CIOs job ever, ever, ever. The CIO to me is an offensive coordinator. That's a term that I take from Tom Kellermann from, formerly of Trend Micro. He now has a VC for security stuff. CIO is offensive. They are going out and they are looking how to utilize information to better their business, the big data side of it. The CISO or Chief Risk Officer or whoever that person is that's responsible for security, that is a defensive position, in my viewpoint. Currently, the defense dangerously reports to the offense. On a board level structure, the CIO's probably sitting at the table and the CISO is probably not or if so, it's a relatively new thing and they're not as much listened to.

[00:25:00] Those people have two functions that do not necessarily come to the same conclusion. Obviously you have to have in both of those positions business minded people who understand that it's a compromise between the use of information and the protection of information. You have to have both voices at the table, in my opinion. When an executive says they don't see the CIO as having that position, I'm with them, but it's for a different reason. It's because I see a separate. In the average corporation now, I don't care if you're a business of ten or a mega corporation, multinational, of hundreds of thousands, you've got to have somebody that is representing the voice of security. The person who's representing the voice of more and more data is not meant to be that person.

Bill: I would agree with you. I think that the bigger the company, the more that's happening. I see it happening more slowly on the small to medium, which I think is the reason why you're opinion is, it really needs to be heard because it's not happening at the lower, at small to medium business as fast as it should. Would you agree?

John: [00:26:00] Yeah. Nothing does because we're all of us small businesses, entrepreneurs, medium, we're just serving in every position. Let me give you a good example of how you solve that. By the way, everything we're talking about in my estimation has a solution. The whole fear, too much fear about this, we can't win, deer in headlights. It's got no place if you're taking some really smart steps. For the entrepreneur out there who's listening, for even a medium sized business, you can have a CISO that is external. You can have a tech person who knows about penetration tests, who knows about doing a cyber audit, who sits in your once a quarter, once a year meeting and represents security, the security perspective. Do you have to trust that person? Of course you have to vet them. Of course, just like you would an employee, but you don't have to necessarily have to have him on staff three hundred and sixty-five days a year to have security represented on your board.

[00:27:00] What I see in a lot of companies now, and heck, my company is one. I took one of my businesses over from my parents. I'm the younger kid. I'm the one that was versed in some technology. Guess what, I'm the one that gets to head up security and be the one that makes sure that we bring in an external security audit and get the firewall set up. Do I do it all myself? No. Do I hire some external? Yes. There's no excuse there for not having that voice in your executive team.

Bill: I would agree with you. I don't think people understand. I call it a rent-a-CISO. You can rent it. You can rent that service. I don't mean to belittle the word rent, but I think you can, like you were saying, you can take it on fractionally, because some people don't have a hundred and fifty thousand, a hundred and seventy-five thousand a year to spare with a fully vetted and trained CISO on staff.

John: Yep.

Bill: [00:28:00] I like your perspective on CIO as an offensive role and the need for a defensive role to emerge that reports up through RISK or reports directly to CEO or to COO for example. I love that perspective. As far as building a culture of privacy, what other elements to privacy and building a culture do you see within an organization being relevant to having to come from the CEO or having to come from the board of directors? Is there anything that's critical to building it that CISO or the CIO can't do themselves, they just need organizational support for?

John: [00:29:00] Yeah, absolutely. I mean, first of all it starts with the executives. Think of the Sony COO emailing username and password and so forth through the system and setting up that culture. I have to say, if you don't have, if you haven't built the team around you, and by the way, these principals are going start to sound repetitive and that's because they are totally repetitive. The buying in of a team beneath you that implements it and that is excited about security, not psycho, not fearmongering, not it's got to be my way or the highway, but, "Hey, let's sit down and have a conversation as manager/worker and an awareness session. You know what, let's get your mobile phone protected. Did you know sixty percent of you right now, don't have a pass code on that? Let me show you how I can get into your bank account in forty-five seconds, since you don't have a pass code." That's something that I do in my presentations. Guess what, when they can get into that bank account, they can also call as you into the office. They can represent themselves as you on email because you've got email on that smartphone. They can take over that email account.  
[00:30:00] You bridge from that, again, from that personal to that private. The CEO sets the tone, the CEO is the one that when they talk about it at the annual meeting, when they get it up and they say, "This is important," and then they bring in a speaker or they have some sort of topical focus on security in general, it shows that they're putting their money where their mouth is and that sets the tone. All the real work is done down in the trenches. The people that I work with are generally the IT or the security team who need to send the message more broadly, even beyond what I do, that's where the real work, because this is all about building excellent habits. This is like within [Alkoa 00:30:35], worker safety. Well, when you have excellent habits of detecting social engineering, the whole equation of manipulation and deception changes.

Bill: [00:31:00] One of the objections I hear about CIOs or CISOs that want to start educating the user community is generally the CISO is not very powerful in the organization and even if the CIO is more powerful, they're finding they have to go talk with HR. Then now this is an HR issue. You sort of now if they listen to John Sileo speak, they come back, they're fully empowered to start educating employees about cyber risk and giving them practical, useful, personal information to help reduce risk with the company. Now they got to run it through HR and go through, now it's like a dead horse they're carrying on their back. How do people get around that?

John: [00:32:00] By cooperation and compromise and by a leadership team from the board down through the CEO down through whether it's the CIO, CISO, that says we are doing this. This not optional. Again, that's why when I recommend where a company start, I want to have that board buy in first because when they say this is now an initiative and HR, you will be the ones at fault if this initiative isn't carried out at the most detailed level, obviously this isn't stuff that happens at the conference. At the conference, you generate interest. Inside of the corporation, inside of the Pfizer or inside of Northrop Grumman or inside of these companies I've been inside of, the hard works happens after I walk off the stage and they're left with the task.

[00:33:00] Take a gander of one of the public retirement systems I worked with. Phenomenal implementation of this. It's because they've got forty billion dollars under management. They're not a highly profitable company because they are about public retirement, so they don't have all kind of extra money to spend. What do they do? They do regular lunch and learn, half to be there, you get two or three options in the week to be at one of these seminars and that's what generates interest. Then they utilize the technology like Wombat or something that helps train on phishing schemes, on social engineering. It takes the basic themes that they've heard in the energy session and it turns it into kind of an automated version of, "Okay, now I care. Now I'm going to click through this and I'm going to pass the test." Then, there are cultural incentives.

[00:34:00] Here's one of the things that gets missed all the time. We'll incent our sales people to make a sale and make a ten thousand dollar profit. By God if we'll incent the whole team for saving us a billion dollar target like breach because we protected the data. There's part of the culture there. If you as a business go through and you don't have a major incident, your team is doing something right, because everyone of you right now is being attacked and penetrated in some way. If you don't have a massive incident in a year, you should celebrate your people. You should reward your people and incent them to continue that behavior. It should be at the highest levels that that recognized. On the walls of this public retirement system, it had pictures of the employees who had a zero percent phishing click rate. It had a chart of, "Listen, we went from six and a half percent of clicks to less than point one percent of people of clicking on phishing. By the way, the technology picked up the other point one percent." That kind of championing and blowing the horn when there is success and rewarding it, it's huge in terms of the cultural belief.  
[00:35:00] You walk into a company like Google or Facebook. You see somebody having to log in with two factor authentication before they even get on their machine. You say, "Why are you doing that?" They say, "Because we're protecting our surfer's data. We're protecting our user's data." They already understand that that's their job and their responsibility. That's because they've been properly trained. It's consistent. It doesn't have to be expensive. Much of it can be automated. It's constant. Every year they have some sort of training on this type of topic.

Bill: [00:36:00] I love that point you just made about rewarding because it's interesting. The senior VP of sales comes into the CEO and says, "I'm going to deliver you seventy million dollars in sales this year from all these various channels. I have a plus or minus five percent, two and a half percent likelihood of that event happening plus or minus, there's a variance one way or the other." They're promising this much revenue for the organization. If you miss that target, if you achieve that target, there's celebratory parties. They send the sales team to exotic locations. There's a lot of- If you miss it too many times, the senior VP's gone. It's interesting, you make this point because the quiet service like IT, the quieter and the more calm [inaudible 00:36:16] are the less people are running down the hallway saying that their computers are broken into or they're too slow. Quietness is actually success. Nothing happening is actually success.

It's almost like they need a set of metrics to say, as you were just pointing out, "What defines massive success? With the variants you give me, within that, so that it's very much equivalent to the senior VP of sales would have a conversation with the CEO about."

John: [00:37:00] Yes, if we could get people leaders to think in that way, to think of security as business as usual, to put it on a plane with legal and sales and HR and just have it be part of the business and therefore incent and reward and by the way feedback and when somebody fails multiple times, they're let go or they're reeducated first and then let go, whatever. That type of perspective on this would cost so much less than responding to the breach post-event. It makes an exponential difference to slowly start accumulating this security and this privacy in your organization as a culture.

Bill: You mentioned that you like to rock climb. Do you still rock climb?

John: [00:38:00] I don't do much rock climbing anymore. For one thing, I lost my partner. I also lost a lot of trust in knowing the person who's below me. When I'm with my daughters, yeah, I rock climb, but in general, I've switched to snowshoeing and mountain biking and hiking.

Bill: Oh, fantastic. Are there any particular, I know when I run and when I find there's a direct correlation, it's almost like a math equation, the longer I run, the better ideas flow into my head.

John: Oh, no question.

Bill: Do you find ...

John: My creativity.

Bill: Does that happen for you as well?

John: [00:39:00] Yeah, in fact, I have, sometimes, I have to force myself. I get in the mode of sitting in front of my screen and responding to emails. All of this stuff that's important, but it's not, there's no actual transformative change there. I'll force myself to take my snowshoes, to take my hiking boots or whatever and it's at about mile three or four of when my brain kind of shuts off and it starts to work its magic and actually think through things in a much more creative, broader perspective than if I'm actively trying to think through something. That's- Some people get it in the shower. Some people get it on the bike or in a spin class or whatever, but what I know without question is when I'm in a patterned behavior, it could be walking, could be hiking, could be biking, my brain works in a totally different way.

Bill:[00:40:00] It's interesting, there's a lot more research coming out on breathing and I know there's all sorts of people talk about breathing and you must breathe and there's yoga breathing and there's people talk about runner's high and things like that, but there's actually like a lot more science coming out because we have more powerful tools for understanding what's going on within the brain and the release of different neurotransmitters that oxygenating the body has an incredibly powerful effect on our whole systems, more than just the tradition runner's high perspective.

John: [00:41:00] That's interesting. I start my day in Colorado here by walking out on my back deck, sitting in a chair, closing my eyes and breathing deep. It just kind of awakening each of my senses one at a time. First thing I do is I smell, for whatever reason, because it's early morning and it maybe just rained or the flowers or the pine trees. Then I listen, then I look and I kind of feel the chair. All of that really is about breathing. On days when I do that, and it's certainly not every day because I fall off the wagon as much as everybody. On the days that I do that, I go into my work with a totally different perspective. I go into how I treat my wife and kids with a different perspective. I think maybe that has something to say about security which is, this isn't about panic. This is about breathing your way through the things you don't do well, breathing your way through the failures and finding a resilience that ultimately is way more secure than having built the highest wall.

Bill: [00:42:00] No, I find a huge link for what you just said. I think it's actually very important for people like yourself and myself to remind people not to panic. The amygdala's a very old part of our brain. It goes back to the beginning of time. I know somebody just saved, a woman just saved her daughter or son from being attacked by a mountain lion in Colorado. That's the old amygdala, with the rustling bush and boom. It's a predator. We think in a digital, the constant chattering things around us, it does trigger that part of our brain. We need to get out of that and into more settled adult oriented, calm approach. Not to say we're not intensely serious and intent. You're so right. I think there's reminding people not to be so panicky is huge piece of this.

John: [00:43:00] I love that we're talking brain science, because behind all of this laughter that happens in an audience and the connections and the interaction and stuff is actually the brain science of cortisol and amygdala and the prefrontal cortex. There's the basis of social engineering right there. If I want to socially engineer you, I'm either, as a woman, I'm going to engender your trust. As a male, I might engender fear and flush your brain with cortisol. What you need to know, is hang on, slow down, breathe deep. That's the hogwash reflex right there. Take a minute to think it through. After about fifteen seconds, you start to think, "Oh, my God. Of course this is fraud. Of course I shouldn't click on this link. Of course I shouldn't give my username and password to this person on the phone. Of course this isn't my grandson calling for money from jail." It's all brain science. If you don't found it in all that we know about how humans work and counteract that amygdala and that response of somebody jumping out of the bush, we're just totally reactive and we never prevent.

Bill: [00:44:00] Exactly right. I think we talked about earlier not poo-pooing the devices and the technologies because some of them are incredibly powerful and useful. I think it's common knowledge now, the human weakness is a big piece of this. This comes to a larger conversation with artificial intelligence, people getting concerned about machines taking over. I think one of the biggest ways machines won't take over is if humans don't panic and actually, from the top down, start to lay out a strategy of how to approach IT security, which is linking it very much to like VP of sales. I think this comes back to the CIOs and the CISOs as even a younger profession. I'm sure you know the data on this, but when was the first CISO landing in the corporate America? What '04? 2004? When was the first VP of sales?

John: Yeah. Prehistoric.

Bill: Prehisto- Yeah. Mesopotamia? I mean. We've had a long history of VP of sales, we need to mature that CISO role a bit faster.

John: [00:45:00] I think you an I can probably both count on having our jobs for a long time because it is new and it's not going away and AI and the internet of things and robotics and having every device connected. There's a hard trend to Dan Burrus. That's a hard trend that's happening with or without us. It's how we react to that and how we think strategically, which is sorely missing from most corporations, certainly from smaller and medium ones, how we think strategically about this. Like you say, stay calm, keep calm and think through how do we build in security? How do we think about these issues when it comes to AI and robotics and the internet of things.

Bill: [00:46:00] Let's get real practical for a second. You have this awesome blog post. Actually, I hit your site and I read three. Maybe we'll only pick on one. I want to pick on ransomware because it's very technical, yet at the same time it has a huge social piece, which I think links a couple, a lot of our discussion as we start to wrap up. What I like about this piece is you actually get into practical steps towards the end. I would love to get your perspective on data classification. Someone clicks something they shouldn't have clicked and now we have an event called files are rapidly being sucked up and encrypted. You, I want to talk to you about data classification. How could a company reverse engineer this so that they would be better prepared to handle randomware event happening? I think ransomware, for a lot of people is not a question of when, or if it's going to happen, it's when it's going to happen.

John: [00:47:00] You bet. When you reverse engineer it, you understand that there are essentially three things that you have to look at. You've got to look at the human response of clicking on a link or going to a website or opening an attachment on an email that they shouldn't. There's the technological side of detecting it, whether it's in spam filters, phishing filters, intrusion detection, that kind of thing. Then there's the old fashioned and terribly effective real time, off-site backups. The cloud has made that certainly more available. It's also there some security issues with backing up in the cloud. If you take a look at these hospitals that have been hit in the last six months, that are- This is shutting out life support equipment, not just patient data. When you freeze up the hospital, you freeze up the ability to save lives.  
[00:48:00] The ones that have survived well are the ones who already had real time off-site backups that would allow them more redundancies, machines that they could sub in that would allow them to continue or recover so quickly that they didn't have to pay the ransom. Unfortunately, what we're seeing in the clients that we've worked with is ninety percent of them are paying the ransom. That does nothing but encourage more ransomware, more cyber blackmail. Until we stop that cycle, because we've got a better answer, we have prepared for it, it's gonna continue to grow. It's going to be the new shiny object here in security for the next couple of years.

Bill: You did mention that ninety percent are paying but only fifty percent are actually receiving the unlocking key. I never heard that. Oh my god.

John: [00:49:00] Yeah, there's no guarantees. These are criminals. The funny part is, even fifty percent, in some cases you are receiving better customer service from your ransomware provider than you are from Comcast. Right now, I just saw one this morning. They've got a chat feature with the purveyor of ransomware. You can get onto the lock screen and you can chat with them and learn how to buy bitcoin and pay the ransom and you can pay it all there on the chat screen. Honest to God, this is organized, like these people went to Harvard business school and have learned the lessons of great customer service.

Bill: [00:50:00] This blog post is a nice step by step guide, very accessible. What's interesting, is with what we've found is when someone is hit with ransomware or it's encrypting files very fast, is that you can rent the capabilities. If you're a small or medium business out there that- I think the issue is not that you can't buy the technologies. You need somebody to run it. You need someone to run it well. I think there's an average of forty-six security technologies in most businesses. It's tough to run them all well. You can actually rent that service that will watch for abnormal file opens. You might have a normal pattern of two thousand file accesses a day. If that spikes within an hour to six thousand, you can actually have a system that can alert and block that from happening. You can rent that service from a cloud service provider. There's several out there that do that. To your point earlier, where you talked about renting the CISO capability, we can actually rent that capability as well if we had that desire.

John: Let me tell you where that generally fails so that people can go one step further, because that's an excellent suggestion. Just like Target who had purchased an multi-million dollar system to detect point of sale malware, it detected the point of sale malware and it sent that to somebody's inbox who decided to ignore that particular red flag. It's not just the software you need, it's the person like you said watching it and letting you know about it and turning the systems off or shutting it down before it becomes a major problem. It goes beyond the technology and into how you utilize that technology and implement it in a very consistent way.

Bill:

[00:51:00] People are going to laugh when they hear this, but this is going to dovetail what we're talking about. You can use this story if you'd like. We go through a process for interviewing about sixty different areas for security risk. One is them on an antivirus. People are like, "Why are you asking antivirus questions?" It's like, we don't ask the question, "Are you running antivirus?" Because that's every person on the staff of that company is going to say, "Of course you run antivirus." When you actually peel back the onion and say, "Okay, are you running it in development production? You're running it on your cloud service provider? Are you looking at the exclusions? Are you actually- Is there a process where those exclusions go to your help desk and your help desk is watching for failures of the antivirus running? Do you update it from your maintenance perspective?" There's so many human being pieces to break the process that the human error piece just on simple antivirus can get a skew. We've had some high level IT. The strategy VP of IT is sitting there going, "Oh my god, I don't ask questions about antivirus, because why should I. I'm trying to figure out technology to bring money into the business not worrying about my antivirus exclusions."  
[00:52:00]  
John: Yeah. There's your offensive versus defensive. Look, you've got to look at both sides. The old saw, "The devil is in the details." Boy, in the digital world, that's really where the devil is is making sure everything is operating properly.

Bill: John, we're going to wrap up here, but this has been a fascinating conversation. We've covered everything from neuroscience to your book to some board level conversations to practical execution of educating people. What's the message you want to leave for the audience today that you want to leave people with? You can pretend like your flying to Denver airport and there's a John Silio billboard. What would be the message on that billboard?

John:  
[00:53:00] God. That's a great question. Hire me. The message would probably be, "Don't forget your people." They are, instead of most articles and tech and security publications refer to them as the weakest link, I think of people as your first line of defense as you're greatest asset protection. The people are what differentiate the business. I don't care if it's a tech business or an old style retail vendor. It's the people that make the difference and those who focus on the people will change and will have a competitive advantage. It's all about the people, Bill.

Bill: I love that. I love how you switched it from people, the biggest weakness to people are the advantage. Again, it's a slight but I think it's a much more empowering way to look at it. John, thank you very much. This has been super fun. We finally connected and it's been worth it.

John:  
[00:54:00] Thank you so much for having me. I hope that if there's anything else I can do for your listeners to help out that I can do that.

Bill: We're definitely going to link this show up on show notes page, share it out on your blog as well. We'll amplify your message. It's very powerful and I hope that you can continue to spread it into corporate America.

John: Fantastic.

Bill: To individuals!

John: Thank you so much.

Bill: Take care. Thank you.