uberknowledge

Scott Augenbaum, Consultant, Speaker, and Author

Back to Basics

Scott shares his lessons from 30 years at the FBI. He states that 90 percent of cybercrime could be prevented with simple user education and cautions us all to know what our children are doing on the internet.

02:20 Nobody ever expects to be a victim of cybercrime. From large companies to individuals, too many are misinformed and underestimate the threat.

03:53 The bad guys do not care who you are, they just want the information you hold.

04:11 The bad news: The bad guys will steal your stuff, law enforcement won't be able to retrieve it, and they won't be able to catch the bad guys.

06:10 The good news: 90 percent of incidents could be prevented by simple user education, well-defined business processes, and two-factor authentication.

09:36 The more money we spend on cybersecurity and prevention, the more cybercrime there is. We're just not doing this right.

13:24 Organizations do not understand the lack of sophistication that is required to pull off a major financial cybercrime.

15:16 Being compliant is not the same thing as being secure.

18:39 We need to train people on the risks and simple cyber protections at home because then they will bring those habits to work.

19:36 When an employee becomes a victim of cybercrime, the enterprise suffers too.

21:26 FBI versus FBE — somebody has to teach the basics.

24:19 Cybercrime extends beyond the corporate world to somewhere even more precious: if something happens to your children online, you can never get their innocence back.

Ashwin Krishnan: [00:00:38] Another edition of the UberKnowledge podcast and a really interesting guest with me this morning. I'll just name the name because his background is so interesting, I want him to do the honors of talking about who he is and what he does. So with me today, I have Scott Augenbaum. Scott, do you want to introduce yourself to the audience, please?

Scott Augenbaum: [00:00:59] Yes. Good afternoon, Ashwin. Thank you so much for having me. My name is Scott Augenbaum. I recently retired from the FBI, about 15 months ago. I spent 30 years with the FBI — twenty-three years as an FBI agent and about half of my career spent in the investigation of cybercrime. I spent the majority of my time in Nashville, Tennessee and Washington, D.C. and during that timeframe I had the opportunity, unfortunately, to be involved with thousands of cybercrime incidents in my career. And the past 15 months, I've been spending my time going around the country speaking at conferences, educating organizations, and recently I wrote a book called "The Secret to Cybersecurity," which is a simple plan to protect your family and business from cybercrime.

Ashwin Krishnan: [00:01:57] Excellent. Let's start with the book. So, two questions: what was the driving force, what prompted you to actually write the book, "The Secret to Cybersecurity"; and the second follow-on question is what would success look like for Scott if X happened as a result of the book being published?

Scott Augenbaum: [00:02:20] Well, two great questions. Why did I write this book? Well you know, during my career I went out and I had the opportunity to get in front of a thousand cybercrime victims and in each one of these situations they always fell into the same four categories, which I call the four truths. The first one was nobody ever expected to be a victim. Every victim always said prior to this, "I don't have anything that the bad guys want. I'm a small business, I'm a nonprofit organization, I'm a real estate company." In Nashville we have a ton of healthcare companies and they would all say, "Well, we're not as big as the big boys. We're not as big as HCA or Community Health Systems." And I would say, "Well, how many records do you have?" And they'd say, "We only have 70,000." Ashwin, come on! Only 70,000 records! There was a lot of information.

[00:03:20] And then I would hear it with the publicly traded companies. The publicly traded companies would say, "We're on the Nasdaq. The bad guys are only targeting companies on the New York Stock Exchange." I've sat down with publicly traded companies that have a net asset value of close to $8 billion. You know they say, "The bad guys are only targeting companies with $10 billion and above." And I'd want to stop and say, "Where are you getting this information from, People magazine?"

"Nobody ever expected to be a victim"

[00:03:53] This is so important. The bad guys do not care who you are. They want the information that you have, and we have all of these different platforms that are out there storing sensitive information. That was the first driving force. Nobody

ever expected to be a victim.

Ashwin Krishnan: [00:04:11] Yep!

Scott Augenbaum: [00:04:11] Then it would go up to point number two. When the bad guys steal your stuff, and let's think about it, Ashwin, what do companies have that they want to steal? We have money, we have intellectual property, we have HR records, we have our Salesforce accounts. And the hardest thing that it took me to get victims to understand was when the bad guys steal your stuff and you contact law enforcement, the chances of law enforcement getting your stuff back is slim to none. I hate to say that. And in a lot of these large data breaches that I've worked on in my career, we were the ones that were telling organizations that they had a problem. Now you think it's a bad day when you have to make a decision to call law enforcement. Do you know, Ashwin, what do you think the reaction was of an organization, when I would knock on their door and say, "Oh by the way, here's your stuff."? How do you think that went?

Ashwin Krishnan: [00:05:09] I can only imagine!

Scott Augenbaum: [00:005:13] It didn't go very well.

Scott Augenbaum: [00:04:38] And then the third point is the chances of law enforcement putting the bad guys in jail are very challenging because where are the bad guys? The bad guys are located overseas, right. They are located over in Asia. They are located in Russia. They are located in West Africa. I want to talk about the business email compromise. So, let me ask you; let's take these two points that I'm really going to reiterate. The bad guys steal your stuff. Law enforcement isn't getting it back. The chances of putting bad guys in jail are challenging because the bad guys are located overseas. So let me ask you, how does that make the average person feel? How do you feel now that I just said that to you?

"90 percent … could have been prevented through basic user education"

Ashwin Krishnan: [00:06:01] I feel we're completely unprotected. We are living in a delusional paradise, and when the shit hits the fan, we don't know what to do.

Scott Augenbaum: [00:06:10] Yeah that's a great answer. And you know what I feel, I feel depressed. You want to know what I feel depressed about? What if I told you that almost 90 percent of what I've dealt with in my career could have been prevented through basic user education and awareness, well-defined business processes, and using two-factor authentication on every bit of remote access. So that is what drove me to write this book because so often when I would sit with an organization and I would see someone's life destroyed, and they weren't getting their stuff back, we weren't able to put somebody in jail, and then what was I going to do say to them, I know your life is destroyed but all this could have been prevented? And that's why I wrote this

book which I define more as a passion project of my own, which is to get in front of as many people as humanly possible to share my experiences as an FBI agent, so they and their family and their business do not have to become the next victim.

Ashwin Krishnan: [00:07:25] Wow, wow. So, I have to follow up with that because this is bigger than just cybercrime. You're actually taking the learnings — and I'm referencing back to your LinkedIn article; I think you wrote it at the time you were leaving the FBI — which is it's time to follow your passion and say goodbye to the FBI. Now for most people, and this is, I guess it's larger than cybercrime because a lot of people very rarely have the privilege but also, I'd say, the courage to follow their passion. In your case, like you said, it was it was obviously very personal to you. I can sense that about dealing with these cybercrime victims and being able to offer very little in terms of either renumeration or solace because their lives have been destroyed and now you've taken that on as a challenge to yourself.

[00:08:18] So, we've talked about the vendor community in the past, you and I. We've kind of looked at it and always had this big question: what's the incentive for a vendor to go to an existing customer and say, "Hey, you know what? I'm going to help you use the product you currently have and make better use of it, so you don't have to buy anything else from me, but you might get more secure."? There isn't any incentive for any vendor to do that. I mean the spending is only going up, the number of cybersecurity companies that are getting funded is only going up, yet we are not feeling any safer. So how does Scott reconcile himself to the fact that you are definitely following your passion and you're making an impact to the world obviously, and yet we have this larger universe of the vendor community which doesn't seem quite aligned with the need or ability to solve the problem?

"The problem is going to increase 100 percent in the next five years."

Scott Augenbaum: [00:09:15] Well, one of the things that I do when I get out in the community and I'm speaking at the IT conferences — you know my job is also to go out and educate the community — and I bring a couple of facts together that show the cybercrime problem is increasing. According to a great article by my good friend Steve Morgan from Cybersecurity Ventures, this cybercrime problem is a $3 trillion problem going up to a $6 trillion problem. OK. So the problem is going to increase 100 percent in the next five years. That's pretty scary. But according to the research today, we're spending $88 billion on keeping ourselves safe. We're spending that on hardware. We're spending that on software. We're spending that on consultants. We're spending it on being compliant. We're spending it on cybersecurity training. But in the next five years, we're going to go up and we're going to be spending $1 trillion, which is almost a 1,200 percent increase. So, what does that mean, when the crime problem increases and the money we're spending on controls increases? It almost seems like there's an inverse relationship and that makes no sense whatsoever. If I would try to explain this to my 13-year-

old, you know what he would say? "Dad it looks like the more money we spend on tools, the worse the problem gets."

Ashwin Krishnan: [00:10:48] [Laughs]

Scott Augenbaum: [00:10:48] So what does that mean? In my opinion it means — and I say this and I'm waiting for someone to challenge me — it means we're not doing it right. Do I have the answers to say what is right and what is wrong? All I've had in my career is the opportunity and misfortune to get in front of a thousand victims and to be able to figure out that in most of these cases they weren't doing the basics; they weren't doing the fundamentals; they weren't, at least on the technical side, following what I like to call the core critical security controls, and they did not understand the threat. So, that is my calling right now to go out there. Unfortunately, sometimes what I talk about isn't very popular these days because I always say if someone's coming to your door and they're trying to sell you a solution that's going to solve all your problems, don't let them in. There's no such thing. Cybersecurity is not easy. And all I am saying is you need to do the basics and the fundamentals first because if you spend money and you don't do that, you're still going to have a problem.

Ashwin Krishnan: [00:11:58] So Scott, let me ask you this, given that you do a lot of this talking, engage with a lot of practitioners as well as vendors, is there a human side to the equation as well? If I'm, let's say, a cyber ops specialist in a large financial organization, I need to understand ransomware or I need to understand how, I don't know, how bitcoin works, how hacking works, etc. Therefore spending time, like you said, and implementing MFA or spending time making sure that my CVEs are well taken care of isn't something that's actually resumé building. More importantly, it doesn't give me the kicks of really understanding what the bleeding-edge tools are, the tools of choice the bad guys are using.

[00:12:51] So do you see some kind of dissonance in terms of the human side of I need to understand the most cutting-edge technology out there just because it gives me the goosebumps versus, like you said, the basic hygiene and good business processes to make organizations more secure? So that's one part of the question. I think the second part of the question is do you see regulations playing an important role here, or do you still see them as just a kind of a checkbox item where you have to fill it up and move on?

Scott Augenbaum: [00:13:24] OK. I'm going to answer your first question with one sentence. Organizations do not understand the lack of sophistication that is required to pull off a major financial cybercrime. We're spending so much time on technology issues, but we're not looking at basic business processes within an organization. We see that every day that I go out and talk to an organization. If I sit down with the C-suite, and I ask them, "What is the most important piece of information that you need to protect?", if I ask 10 people that question, how many answers would I get? Then I will go through very basic, simple platforms that they all have within their organizations. I'm asking them things like do you use two-factor

authentication on your payroll. And they'll usually go, I got to ask the CFO. And then in most cases the CFO goes, "What's two-factor authentication?" Think about this, what could the bad guy do if he gets the administrator's account for the payroll at a large organization? He can divert the complete payroll account. It's simple. We can lock that up. Then we'll go over and ask, "What are you using for your HR platform?" "Well, we're using Peoplesoft, we're using Workday." "Well, is that secure or is that locked down?" "Well, let me check with the director of HR." There are all these platforms or we're dealing with Salesforce. What do you think a bad guy can do if he gets into a Salesforce account at an organization? He has access to all the contacts or even the email. So we have to really identify those things first.

[00:15:16] And whenever you go over and you look at all these traditional regulations that are out there, such as HIPPA or Hitrust or PCI or SOCKS, being compliant is not the same thing as being secure.

Ashwin Krishnan: [00:15:30] Yeah.

Scott Augenbaum: [00:15:31] So those are the two really basic things to just try to answer those questions. Look guys, it does not take a lot to be able to do that. And I have stories that will blow your mind of really easy things that organizations could have done to protect themselves, but they were spending so much time trying to protect their network. Now we don't know where the network ends because we're using mobile technology, we're logging in remotely from our home, and we're logging into a system where now we have access to the Crown Jewels.

"Now we don't know where the network ends"

Ashwin Krishnan: [00:16:09] Yeah. So extending that argument forward, whether it's 2FA, whether it's using a rotating password, the question that it comes down to — and again you mentioned the financial organization, you mentioned HR organization — so, from a company-wide security-culture perspective, what sorts of success stories have you seen? Stories where every employee in the organization regardless of function, hierarchy, title or whatever, he or she is aware of what a phishing attack looks like or why a 2FA would take another extra 10-15 seconds to be able to log in, like you said, to a Peoplesoft or Workday account, but it's worth it. And have there been best practices; has there been a resurgence of why this is important, and how has a successful organization been able to imbibe that security training or culture in the length and breadth of the organization?

Scott Augenbaum: [00:17:14] Well you know, I can only measure the success in the past 15 months. I've been hired a thousand — not a thousand — I've been hired a lot because I don't sell anything. When I go out and I'm training a healthcare organization, and a CIO comes to me and says, "Hey I need you to train my folks because they need to understand HIPPA." I go, "That's a waste of time," and they all get taken aback. "What do you mean that's a waste of time?" I said, "If you can

teach your employees how to be safe at home, so they understand that on December 23rd when they get an email from Amazon saying that their package has been delayed in shipping, if they click on that it's probably from a bad guy who's going to infect them with either ransomware or a keystroke logger, and you can take those stories and you can make them real life, then you're going to change behavior." Because as I sit out here now, and I look at a lot of these cybersecurity awareness products, what are they? They're a white paper and they're Saturday morning cartoon animation. Which is, what do you get? Saturday cartoons and white papers. We need to be training people on the risks at home because if you understand at home the risks, you're going to take that to your organization.

[00:18:39] But remember the other 10 percent is hard. That is why you need the technology vendors. That is why you need your firewalls, your email gateways. But we have to realize that email is 90 percent of the attack vector. And here's a question that I end up talking about with HR folks all the time. And I want you to answer this as if you were the HR person. I go over and I talk to an HR director, and I ask her is online identity ... no, I'm going to ask you: online identity theft, is that problem getting better or worse? What do you think?

"Email is 90 percent of the attack vector"

Ashwin Krishnan: [00:19:15] Worse.

Scott Augenbaum: [00:19:17] OK. Is it an organization's responsibility to train their employees how not to be a victim at home?

Ashwin Krishnan: [00:19:25] No, I think ...

Scott Augenbaum: [00:19:28] In theory it might be, but do most organizations train their employees how not to be victims at home?

Ashwin Krishnan: [00:19:34] No.

Scott Augenbaum: [00:19:36] Of course not. Nobody is saying they should because they have way too much to do. How many hours do you think it takes for an employee at a publicly traded company, if they become a victim, how many hours do you think it takes them to fix that problem?

Ashwin Krishnan: [00:19:53] I have no idea, but a lot.

Scott Augenbaum: [00:19:55] It does take a lot, right.

Ashwin Krishnan: [00:19:58] Yeah.

Scott Augenbaum: [00:19:59] When do you think they take the time and fix that problem? Do you think they do it at home at night or on the weekends, or do they do that on work time?

Ashwin Krishnan: [00:20:11] That's a great question, I assume it's probably work right?

Scott Augenbaum: [00:20:15] Of course. Is that an HR problem or is that not an HR

problem?

Ashwin Krishnan: [00:20:19] It is an HR problem.

Scott Augenbaum: [00:20:20] In my opinion, that's an HR problem.

Ashwin Krishnan: [00:20:25] Now this is this is amazing. So the person who is at home and the employee who's at work, she's the same individual.

Scott Augenbaum: [00:20:38] Absolutely.

Ashwin Krishnan: [00:20:39] And if you can be secure at home and you can bring the same security mentality when you come into work, your risk posture dramatically gets reduced. I mean that's golden, thank you for that!

[00:20:50] I had one final question for you and that's in the definition of success. In one of your interviews, you mention, "In the old days a success for me was putting someone in jail, today my success stories happen when someone calls me up after a presentation I did, and they say they implemented 2FA on their platforms." So how does Scott feel today about the satisfaction, the fulfillment that you get when you have your audience member reach out to you afterwards and say, "Scott, you taught me so much, thank you for that," versus what you were doing earlier; I know this is not a apples to apples comparison.

Scott Augenbaum: [00:21:26] No, no, no. Well listen, when I joined the FBI, if you would have asked me to explain what I did, I would say it was easy: there were bad people doing bad things to good people in my area of responsibility. And I worked with state and local cops and put bad guys in jail. But when I realized later in my career that it was very challenging, if not impossible, to get the money back and it was very difficult to put these bad guys in jail, that's why I went out the last three or four years in my career and I did so many presentations. I had supervisors who would come over to me and say, "Scott, we're not the Federal Bureau of Education, we're the Federal Bureau of Investigation!" And that is why I have taken this so personally in my career.

[00:22:17] And I met with someone yesterday, and she said to me, "You know, when you showed me how to change my password, by doing what you told me, I did that with all of my passwords." That's why I wrote the book, to share what I've learned because there was nothing out there that was really simple and easy. And the best book review I got was from my sister-in-law, who when she heard about my book said, "This is going to be boring; it's not going to apply to me." And she used it, and she changed things. Because let's stop and think about this, I've been trying to change corporate behavior for decades, and it hasn't really worked. So my goal, Ashwin, is to make sure that I can teach individuals, end-users, senior citizens, and even parents how not to be the next cybercrime victim. That is why what I do. I call it my passion project.

Ashwin Krishnan: [00:23:19] Now this is quite inspirational. I am sure the audience will get a big lesson from this. Just the learning of you can go in and talk to these

people, and once you change the way they think, that's who they are. Whether they influence their colleagues at work, whether they go on to influence their family members, like you mentioned, I think that's how the culture changes. So this is super, super interesting.

[00:23:47] Any last words? I know you've been out of the FBI for 15 months. You've been doing the speaking tour; you're obviously doing the book tour; and you're doing a lot of consultancy. If you had any final words for our listeners, what would those be? I mean you're addressing an audience of obviously enterprise listeners but also consumers who are also people at the end of the day. What would those last takeaways be?

Scott Augenbaum: [00:24:19] If you're the victim of cybercrime it's going to be painful, but you're going to get through it. Make sure you know what your kids are doing on the internet before you go out and you invest the money and you give your children an iPhone. Realize that there are a lot of bad people out there. We're giving our kids very, very powerful devices without knowing the full potential. And I addressed that also in the book because I've had to deal with that. There's cyberliability insurance, but at the end of the day when something happens to your children, you are never getting their innocence back. So let's forget about the corporate side, that to me is the most important thing.

"When something happens to your children, you are never getting their innocence back."

Ashwin Krishnan: [00:25:07] Absolutely, and you're right. I mean, once it gets personal is the point when, unfortunately, the wakeup call happens, and sometimes, like you mentioned earlier, it's too late. So Scott, this has been a really, really interesting and, I think, eye-opening discussion for me. I think absolutely the audience is going to get awareness out of this. And I think your book is going to do really, really well just because, like you said, it's back to the basics and just getting awareness to the masses out there.

[00:25:36] So Scott, thank you for your time and looking forward to further conversations in the future as well.

Scott Augenbaum: [00:25:39] Yes and thank you. It's been an honor to be on your podcast today. Thank you for taking time out to talk with me.

Ashwin Krishnan: [00:25:46] Thank you, Scott.