Ep.29 Can Training Reduce Cyber Attacks on Federal Sites?

SUMMARY KEYWORDS
training, people, ransomware, organization, roi, train, malware, eric, affiliates, phones, years, tools, effective, big, attacks, called, simulated, phishing, security, company

00:04
This is John Gilroy from the Federal tech podcast.

00:06
And this is Eric Crone.

00:09
Today we're going to talk about cybersecurity training for the federal government hit the music clog Welcome to the federal tech podcast. My name is John Gilroy and I will be your moderator. Our guest today is world famous Eric Krohn. He is officially the security awareness advocate for a company called no before

00:31
Eric, how are you? I'm doing great, John. And I love how you elevated me to world famous I can now put that on my resume or CV. That's great.

00:39
Don't worry, the bill will be in the mail. It's a big bill to tell you that much. Now, Eric has a voice for radio, and I've got decades of radio experience. So I compulsively have to spell things out. Because people can listen to this. They're walking their dog. They're jogging, they're washing their cars, something. And so the company we're talking about is no before k n o WB e then the numeral four.com. Is that correct? Eric? That's absolutely right. Good, good. And if you have your little keyboard out, and you type those little numbers anyway, but no, before, you will get a cornucopia of stuff. I mean, if you're bored to know, before, they have free tools, I can't even write down the number of free tools. They have all kinds of tools about security, training and awareness. And so we're talking about today, and more specifically, we're gonna focus on the federal government. Now, I actually do research for these interviews. That's shocking. So this morning, I'm reading an article on Axios AX I O 's. And I read it, it's about, you know, handheld devices and security. And then they had this quote, and this is just a perfect quote, the quote says, companies have been investing heavily and keeping bad actors out, then it's both easy to underestimate and under train employees on cybersecurity. Absolutely, they've been so

busy on the front door, that they leave the back door open. It's this is a perfect setup for this conversation company. Investing so heavily and keeping the bad guys out, didn't realize that training can let the bad guys in.

02:13
Yeah, it's you know, it's an interesting issue that we have in technology. And I'm a geek, I'm a I'm a tech guy, John, I love tech I, I do little sensors around my house from my home automation and stuff, right? I am very much into that. But one of the biggest risks we run in cybersecurity is the human factor. And it comes in through the email phishing and the the text message phishing and things like that. And unfortunately, a lot of the people that are in the industry are like myself, they're very, very tuned into technology, and sometimes forget kind of the soft side of things, the human side of things, because it's not the place that we're normally drawn to. I don't know any cybersecurity professionals, honestly, that took a cybersecurity job because they would be able to train end users that's just not there. That's not our comfort zone. And so we tend to rely on technology a lot more than we should sometimes. And then the front door is just kind of are the backdoors, you put it just kind of sitting there creaking on the hinges a little bit open. And that's the way that the attackers seem to get in over and over again.

03:20
When it comes to the federal government. They're no stranger to the idea of of or the concept of security training. I mean, in fact, basic street training is mandated. Everyone listening to my audience knows what CES is, you can go to the CES site, and you'll see strong suggestions or training. It's almost like, Yeah, I'm training for the Boston Marathon. Everyone should train. What are you doing, John? Oh, I'm getting some donuts at noon. Go to a winery this weekend? Oh, wait a minute. I mean, you can hear the strong suggestion. But then there's a reality. I think this is just the whole thing. So that's what no before is all about. It says, Look, we can help you with this training. And it's effective as well. Is that

04:03
right? Absolutely. We have a security awareness training platform. And then we also do simulated phishing, which is kind of a it's misunderstood. Sometimes people think the simulated phishing is designed to trick people. And that's not what it's about, really, it's about augmenting the training. So they do the online on Demand training. And then they get to practice that with the simulated stuff. But the the key thing here is a lot of organizations do the education piece wrong. You talk about some of these, you know, like NIST and all these standards and regulations, and mostly what they come out is they say you're required to do some, some training, some security awareness training, and then you do it like once a year, you throw a bunch of people in a room, you bore them to death, you throw some coffee and doughnuts at them, and then we're surprised when it's not very effective. So that's kind of what we're trying to tackle is let's make it easy to do and let's make Get a lot more effective than just something like that. The federal government unfortunately, I spent some time there, I was the security manager for the US Army, second regional cyber center Western Hemisphere. We had to undergo that annual training, it was put together by DISA. And I can tell you the first year it was, it was pretty cool. It was interesting. It was different. We had to go clear classified stuff from different rooms, the fourth year of doing the same training, there were cheat sheets that went around with all the answers to the questions and nobody liked doing it. It was just repetitive, old and boring, and very ineffective. That's, that's a problem we run into, especially on the federal side.

05:41
I am a very experienced technology person. So I've seen a lot of things over the years. Now, when I first heard about your company, this is something a little Brainworks Okay, Eric's gonna get in his little car and drive over to interior and go inside and get old meeting room and gather everyone just like gather everyone around, maybe get tell some bad jokes, get some doughnuts go in, and then board one to tears and go home. I mean, so. So this, I hope this is how you do it this way I would do it. But how do you do the training?

06:09
No, I do tell bad jokes whenever I do training. So you have me there. I don't know if somebody leaked that or not. But no. So we do some in house training for like the large enterprise customers, and especially around October, which is National Cybersecurity Awareness Month, there, we actually do some in person training, most of what I do is I actually train other professionals or I educate like board members and things like that more than typical employee training. But our on demand platform has the employee training in there, so they can take it whenever they want. You don't have to get them in there. And what I like about it is we have like 1000s upon 1000s of different types of training available, different flavors, different fields. Some of them are live action, there are people, you know, speaking, some of them are animated, some of them are our games, things like that, that every organization has its own culture internally. And things resonate differently within it. Like I wouldn't provide the same training to a large law office that I would have Silicon Valley startup, it's just not going to gonna fit. And so we have all of those options there. Now, of course, if I do in house training, I'm going to customize it to that audience, depending on who it is. But for the most part, what we found is it's incredibly effective to give them short amounts throughout the year through an online on demand service, as opposed to having somebody come in and just stand in front of them.

07:43
That's good. I, I read stuff. I talk to people, you know, I listen to a podcast or in town. It's called doctors, zero trust. And he's a doctor Dr. Face Cunningham. He a wonderful guy just listened to podcasts yesterday. And he, when he talks about training, he says, you can you could take a PhD and trainer for 10 years, or pay and train him for 20 hours a day. And there's always going to be 4%. They're going to get suckered in. Always. Yeah. And so I said, that's interesting. So I'm listening to another podcast and reading about this guy in Texas. And in Texas, he says, Well, there's a division there whose leaders all flipped out about fishing, because they're getting hit like 34 35%. And they enacted a training. And after the training, they're down to like seven or 8%. And they were jumping up with joy, because seven 8%. So So is is getting it down to a reasonable is that the goal here or I want zero or nothing, it just doesn't seem reasonable doesn't

08:43
know it's not and and I don't agree with the numbers, you know, okay. 5% click rate. Yeah, there's 5% going to click, but I can tell you right now, even in the example you gave, that's a whole lot better than having like 32 or 30% of the phishing emails being clicked on when they come in, right. There's a huge difference in that. And I've felt that, personally, myself and organizations I've been in, I used to, I used to be part of an organization, we had a lot of developers. And they had a habit of going out to GitHub and all these places and just grabbing

stuff and downloading things all the time. Clicking on them, I was busy a couple of times a week, I'm you know, three times a week, I'm rebuilding computers, because they got malware on him.

When we instituted the training program and started getting that click rate down to a reasonable level. That made a huge difference, because now I was only putting out fires and rebuilding machines maybe once or twice a month instead of a few times a week. And that really allowed me to focus on strategic things. So there's a huge difference there. And to the fact that somebody's going to click on things on occasion, that's why we have layered processes and controls in cybersecurity. There is no silver bullet, there's no one thing that's 100% effective. I've had to hundreds of different controls and very expensive security products, and none of them are 100% effective. So you don't want to throw you know, the baby out with the bathwater sort of thing here, it makes a huge difference. And frankly, I tell people with our platform, if you're getting a 0% click rate, you're not making the test one's hard enough. Hmm,

10:21

yeah, that's good. Washington DC is a town where everyone knows everyone, there's certain personalities to the kind of big, there's a personality in town here for many years named Alan paler, because he was selfless. He would come over and change a flat tire in your car, he was just a wonderful guy, he does some things to help me I can't even enumerate them. And he is no longer with us. But he started this whole place called the SANS Institute. So if I am working for let's say, NIH, and I get the mandate, well, you know, we have to look at surgery, I would think, you know, Sans is just down the road. It's just Wisconsin Avenue. And so should should they look at the SANS Institute has something like the well known sans attitude compare with your training.

11:03

So sans does a lot of good, like technical training, I have a lot of respect for their technical training, although the argument that the pricing, we've all heard that argument, it's very expensive. The fact is, they don't focus on the human factor. They don't focus on security awareness, especially and teaching better behaviors and changing culture and changing behavior. They have some security awareness training stuff. That's what we focus on, though, you know, that's our, that's our key thing, we have a lot more options. Like I mentioned, for the training, we have a lot more tools. And our automation is second to none. In the industry, as far as making it easy. I mean, these these people out there that are running these programs, they have about 300 other jobs to do. And so we focused a lot on automating the processes, you set these up, they sent random emails to random people at random times. I mean, our platform is absolutely designed, totally 100% towards doing this kind of training and changing behavior. Sands, although it's a fine institution, their stuff is, is not so focused. And I think there's a big quality difference there. I really do.

12:19

I, I got a meeting. So I started go to meetings after COVID A lot of cybersecurity meetings, get to talk to people and hear different thoughts and everything else. And a recurring phrases defense in depth. And you've heard of dollar defense in depth. While I'm looking at your website, it's like a training in depth like I just one tab is free tools. So I went to K and o WB e numeral four.com. And tools 12345 is the free tools 123456 There must be 20 free tools here they got you know ransomware simulator tool. If you're flipped bought about your team, it's that's that you don't even place a purchase order. Just take and use this tool and play around with it. So, you know, it seems to be there's a whole lot more to it than making sure you have a strong firewall or making sure you have intrusion detection, making sure I mean, all the standard checklist things here. We we forget about the you know, the Born factor the human factor. Hmm,

13:13
yeah, yeah. And you know, that's something that I love about the organization. I've been here about six years now. We started in 2010. I've been here about six years. So I'm one of the early the early people in here. But what I love about it is we're actually really passionate about ending the problem. This isn't an organization that's just in it to make a few bucks and to be a company, if you will. The founder came out of the antivirus space, and he sold his company, Sue Charmin. He sold his earlier company, he had a decent amount of money in the bank. And yet he was still frustrated. See, even with good endpoint protection or antivirus. People were still having issues, they were still getting hit, they were still getting breached. And he said, What can we do to help this problem and that was the founding of our organization, what can we do to help with this problem. And that has just permeated our culture all the way through. So we give away a lot of these free tools. We do. I do a lot of webinars, a lot of my other colleagues do a lot of webinars there. They're all available for free on there, too. We have the white papers, that ransomware hostage rescue Guide, which is fantastic. It gives you before during and after things to do about ransomware and I love it because well I had a part in updating and writing it a couple times. So we keep that one updated. But I love that we provide all that stuff like you said, you just see the free tools out there. There's so much more as well. Lots of good stuff there. You don't even have to pay for it. You never have to pay for it. I love that.

14:46
Earlier in the discussion I talked about my old man image of God walking into a classroom with a whiteboard and talking to everyone. And you know, I would completely forget about mobile. I've interviewed people called lookout I interview a couple of weeks back. And, you know, they just study. And now this is something that boy, I, you know, another shot shocking feger 91% of mobile devices used by federal employees are not managed. Yeah, well, what could possibly go wrong? That's why I'm in that classroom, we get the laptops out and this and that, and this and that. And then they go out to lunch, and they get out their phone and they get hit. Yeah, I mean, I think we have to have this more nuanced approach to understanding. Yes, I think, I think in the federal government, they do tend to have a checklist. And, and yes, we did that yesterday, this yesterday. And they made me forget the more practical aspects of I mean, big, big organizations tend to anyway,

15:43
yeah, mobile is a is a whole difficult side of things here. You know, back in the early days, I've been guilty of this, I had two phones, I had a work phone, and I had a personal phone, but I don't carry two phones anymore, right. And this is normal in the normal world. But the management portions, and I do I love look out I love some of those. It's called MDM, mobile device management. I love that stuff. But people don't want that on their phones, either. Yet, they still want to be able to work. So they want to access email. And there's this crossover that happens just in personal lives these days. And COVID made it worse when a lot of the work from home stuff happened. I mean, we just saw a Cisco breach happened, it was a minor breach. But it happened to because the person was keeping passwords in their Google Chrome, Password Manager, work passwords for that, right. These things happen these days, we have that crossover. And mobile is tough, because it's really hard to hover over a link and see if it's really taking you where you're going or see if it actually came from that

person. But it's a big threat. And that's why we we do focus, we have some focus templates for mobile, we have training on mobile executive stuff, because executives are out there bouncing around all over the place, with their phones dealing with very sensitive stuff on their phones, as a matter of fact, too. And so documents get left behind, they get downloaded and worked on and forgotten about and that becomes a threat. They're also easily stolen, not just phones, tablets, you look at the number of people that use tablets, it's the same thing. They're stolen, they're lost or left on airplanes. Now your data is potentially at risk. It's it's a whole world out there.

17:29

I'm involved in education, my wife's involved in education, and there's all kinds of approaches and and techniques and getting people emotionally involved as I like to do and, and with my students where we go face to face I ever graduate students, we just go face to face and scream at each other. You're an idiot. No, you're an idiot and go back and forth. But when it comes to human beings, you know, if I have a small graduate class of six students, there's gonna be six different ways to hit these kids. One wants to read one wants a video one wants go face to face with me constantly. One wants to text me. I don't know. I mean, I'm in the classroom sexy. So different way to interact. So. So how would you train me not to be suckered in with a phishing attack? I mean, my approach is gonna be different than my neighbor's approach. By the way, he works for the Nuclear Regulatory Commission, so he's way smarter. So how do you regular mere mortal like me and Brainiac? How would you? It's called an education High School is called variable training. Hmm. So how would you do that? Well, it's got

18:29

to be relevant. And this kind of goes back to my earlier example of training a law office versus a Silicon Valley start up, right, it's got to make sense to these people. And if people don't understand how this education affects them, in the real world, if they can't comprehend what this really means for them, then you're not going to have them walk away remembering things, it's not going to make a very big impact. So it's important to understand the generation you're dealing with the types of people that you're dealing with, even down to the departments within large organizations like enterprise organizations or federal spaces. What is the culture of that area? Like? How can we make it matter to them? Now, again, the approach a lot of times is we train everybody on the same thing once a year and call it good. That doesn't work. I really like to see where we take something that's relevant not only to the person but let's say the time of the year. We're going to be coming up on the holidays soon. Scammers are out there. They're in social media, they're they're posting up PlayStation fives for $300. And everybody's gonna jump on it and send them a deposit and Cash App and lose their money, right? Why not take our education stuff and let's focus on even some of their personal issues. Because as they learn to spot scams in their personal lives, they also learn to spot them in our organizational side of things as well. But let's do a five or a 10 minute training on something that matters to them. Hey, how to spot these kinds of scams. You Gonna see next month, or in the beginning of the year, first quarter, they're always after tax information so they can steal people's tax forms, and fraudulently file their tax returns and run off with their money. These bad actors love to do that. So let's train them on how to look for these things using the tax scams as an example, and then people are suddenly interested in it. If you can get the right flavor to people at the right time. It's kind of like the messaging thing, right message, the right people at the right time. They're suddenly interested, they actually want to learn about it. And that's the difference is kind of knowing your audience there and having the ability to provide the kind of training in the way that that really resonates with them. Like you said, you have some people that just want to be face to face on everything. You have some people that, you know, if if you see them once a month, on Zoom, it doesn't matter the rest of the works getting done right that that happens with people. We just need to be able to to resonate with them. I was

21:01
thinking about training, and I'm thinking back on mine when I was young man. When I was about 12, I was had an altercation and I decided to learn judo. And so I bought a book. And I learned all this Rosen's hip bones co Nagi tominaga, Uchi, Goshi Ogu. I know Ma, I was great at the names, and I got whooped again. And so then I found this Japanese guy to train me. He trained me by putting my face on the mat. 1000 times from every direction. I was humbled, but so much more effective than the book. Now. I'm sure there are people that you may read a book and understand the company, but boy, it took me to get my face smashed about 30 times. Oh, so that's okey Goshi.

21:39
And see that? Yeah, that's what I'm saying with the simulated side of things. Now we're not we're not all about smashing faces into the mat. Okay, don't get me wrong. We're actually very much for taking that's the takeaway. Ah, we like positive reinforcement, right? Like, like, we would like to send these people things that are the simulated attacks that maybe, you know, we have a tool out there that actually takes a real attack that comes into an organization, the admin goes, Oh, okay, this is a real attack. This is a campaign that's hitting us, it will actually take the malicious stuff out with it, turn it into a template for us, and they can turn around and send it to the organization and say, okay, because something real is coming in. But it's a practice in a failsafe environment, right? When you practice your judo, odds are you're in some sort of pads, right? Padded floor a little bit. You want that to be a failsafe environment, as opposed to behind the bar at two o'clock in the morning. Right? Yeah. And that's, that's the major difference there. And that's what the simulated stuff is, is about. And I know I harp on that, but it's such a misunderstood part of the training and education programs, that people, they just look at it in a negative light. And that's not how it is at all.

22:50
I think that's the whole idea behind martial arts training is that it's a simulation of the real world. And so you can get thrown in your face and not have major surgery. To bet everyone talks about zero trust is kind of mandatory talk about zero trust. Does this fit and discussion? Do you fit it in with zero trust training? Or is that a whole separate category?

23:07
Well, you know, zero trust is is more about segmentation and things, but this is all part of the layers. When I talk about protecting organizations, I typically talk about all the different layers training and education is part of it. network segmentation, or zero trust type stuff is another permissions on files is another especially with ransomware. If if a person can only read a file, but not write it, they can't encrypt it, right? Little things like that. Data Loss Prevention controls, because they're stealing and exfiltrating data. And then good backups. Those are kind of the layers that I always talk about. So zero trust falls in there, especially in the segmentation side

where you you don't want devices communicating with each other if they don't need to be communicating with each other. That just causes problems like we saw at NHS when wanna cry just ran across. They're very flat network.

24:01
I tend to go to the beach in the summer, and attend to shovel the driveway in the winter seasons here. And so are there seasons for these attacks. Is it Oh, yeah. School starting? And we'll see you. Oh, tax season. You mentioned that earlier that, oh, it's the change of the so are there seasons, are there seasonal? times to be more aware? Well, the,

24:20
the attacks are constantly happening. I think there's no seasons. Yeah, the targeting though is different. And the lures that they use to try to get people into things are different based on the timing. Like I said, the holidays, there's gonna be lots of scams about that first quarter is always tax stuff. You know, it's interesting to see how some of these players work. You mentioned school starting. There are a lot of ransomware players that now what they'll do is they will gain access to a network system like say, for example, in schools and I've seen this and what they do is they wait until like the Friday before the week school starts Ah, that's when they fire off the ransomware because they know that People are going to be out and about, they're taking their last weekend off. We see it in 3d weekends, too. Sometimes, they'll do that when they know that there's not a lot of people around, they can do the most damage, the pressure is on them immensely, because how do you start school if none of the systems work, so they do this even on a micro level with the timing piece, to really push the leverage that they have. I, I don't know if you remember back when, when Trump's inauguration happened down there in DC, but there was a ransomware attack on the cameras the week before the inauguration. And of course, you know, it's been politically charged, there was all that going on there. But a week before ransomware took out like 70% of the CCTV cameras around DC by taking out all the recorders and stuff, and you can imagine the immense amount of pressure that was on the administrators of that to have the cameras up and going during this potentially pretentious inauguration, when we didn't really know what was going to happen, or I was going to turn out, and all of a sudden you're blind, you know, the they do these things to build that pressure. And it's very effective. It's why the cost of ransoms is so high these days.

26:13
No before obviously has a lot of commercial experience. So if you waltz into an insurance company in Chicago, they're gonna pound on the table and go, Okay, show me the money, buddy, show me what's the ROI on this? Because I'm gonna spend $10, on earn and say $10 and make $10. So, okay, don't leave until your tummy. So is there an ROI you give with commercial company? It seems difficult.

26:36
It's a challenge to do. And I'm quoting this off the top of my head. So please don't this is not an exact thing. I believe the ROI numbers we got from I think it was Forrester said it was like a 276% ROI in the first short amount of time he had it. I know we have that information on our website. But there is a huge ROI on this. And mostly because it's not expensive, like people underestimate this when, when I before I came to work here, I

worked in this organization, I was building out the program. And I always made assumptions of what this kind of a program would cost. And I had heard it was expensive. Now, when I came to work for No, before I actually turned around, I called my old boss and I was like, hold on a second. Take a look at this before you spend any more time on it, because I'm shocked at how inexpensive it is. And our prices are listed on our website, too. I think we're the only ones that actually list our prices on the internet. But he looked at it and said, No, you're right, the effort we're putting into it. It's way cheaper just to go this route and have it done. That's something that I personally dealt with was that I underestimated how inexpensive it was. And that kind of bit me in about I could have done better. Had I taken the time to actually not go off my assumptions and look into it a little bit more.

27:57
Well look into crystal ball for me. So where are you see his whole area of training headed in the next four or five years talking about mandatory training? Maybe there's not just mandatory superficial training, maybe there's some going to be some kind of a criteria for this training, where he's headed the next four or five years?

28:12
Well, John, I expect by next year, why have fishing completely eradicated? We won't need passwords anymore. Jared have cancer out of a job, right? I'm just gonna I'm gonna retire, sit on my porch and yell at kids to get off my lawn. That's my goal in life here. No, I mean, honestly, we're seeing the same that more of the same honestly, the attacks are, are bigger, the attackers are getting more mature. And so we're going to have to evolve our defenses to and I don't know if you know this, John, but there's things out there. They have as a service providers for the dark web and for the cyber criminals. So, phishing is a service where they handle the back end, they can send out the emails, you just dump a list into thing. It has a dashboard that tells you how many people opened the phishing emails, how many is viewed them saying it's all this marketing stuff, right? And then ransomware as a service. What they've done here is these malware developers, they develop the malware, they run the back end of things, and they have what's called affiliates. Imagine like the Mary Kay people running around. And they're basically launching these attacks against all these organizations. So the malware developers focus on writing the malware making it good. And the affiliates do the attacks. It's a profit sharing system. Generally, the affiliates get like 70% of the profits from an attack that malware developers get 30%. But it's infinitely more scalable than it was before. So what you see here is this is going to grow, it's going to continue to grow. And we need to battle that by being very serious and intentional in our defenses here. That's what we got to do. We got to continue to be more and more intentional. And we got to wake up and understand that phishing is a huge Huge problem. And we have to take it seriously, we have to understand again, and quit under estimating the adversaries on the other side of this. Where do you set

30:09
affiliate? I flashed on Las Vegas and Blackhat conference at the RSA Conference. And I predict in five years, there'll be a ransomware caught with their affiliates in Las Vegas array of different foods. And Eric will go from booth to booth. I'll talk about well, ours says this.

30:25

You know, there's gonna happen. There's already competition for that stuff out there because these developers want the affiliates to work with them. Oh, yeah, they have. They have specs, like how fast they encrypt, there's actually early on, there was a strain called Philadelphia was $400. To buy into the strain. This is a couple years ago. There's a YouTube video that's a marketing video for for Philadelphia ransomware. Last I checked about a year ago, it's still out there, and it tells you how awesome it is. And it shows you I mean, this is like legitimate marketing on YouTube for a ransomware strain. It's

31:03
401k Medical and Dental. Right. I guess that's what's happening

31:07
in Eastern Europe. A lot of these people they do they work in office buildings like you and I do they have time off? It's structured like a business. Wow. And they're, I mean, they're doing very well if you if you look around, they're doing very well. But that's what I'm saying. It's so much more mature. And sometimes we think that this is the kids in the basement drinking Mountain Dew eating pizza. And this is not what we're facing.

31:33
Difficult adversary. Well, Eric, unfortunately, we are running out of time here. You have been listening to the federal tech podcast with John Gilroy. I'd like to thank my guest, Eric Crone, security awareness advocate for a company called no before. Thank you, Eric.