FEDERAL TECH PODCAST

Ep. 36 Federal IT and the Verizon Data Breah Investigation Report

Welcome to the federal tech podcast. My name is John Gilroy and I'll be your moderator. Today we have Melissa Gilbert. She is the executive director, also the Business Information Security Officer for a small company people don't know called Verizon. Melissa, how are you?

00:31
I'm doing well. Thank you. How are you? John?

00:34
I think if you've been in the federal technology community for 20 minutes, you probably know about Verizon. And if you've been in the federal tech community for an hour, you probably know about this big annual report called The let me get I want to get every single word data breach investigation report, everyone calls the dip or the dip or something like that. What happened is 15 years ago, Verizon came up with this idea to actually study what's going on with cybersecurity and give the give the information away for free, which kind of fascinates me, but every year, people with PhDs, computer science, novices like me, they read it, and they get information for it. What I wanted two days for the benefit of our federal listeners, tee this report up, talk a bit about it, how it was developed, what you do what your role is, so maybe some GAVI sitting over at Treasury somewhere, maybe an interior? Maybe they can benefit from it, because Ryan's really put a lot of money and time into this, haven't they, Melissa?

01:30
Absolutely. Yes. Good. So, roll back

01:34
time. 15 years ago, you're in grade school, and decide to start with this report. So So why did you start it and how do they begin?

01:42
Yeah, no. So So I think it's good. Let's, let's kind of start about how how it all became how it all came about? Yeah. So Verizon actually has an arm on our business side where we provide incident response capabilities to customers, they can leverage Verizon, if they're impacted by an incident 15 years ago, you got to kind of remember where we were right. No one was really talking about data breaches. But it was an increasing trend. And you would hear a lot of anecdotal talk or splashing news coverage about the latest large data breach. And so as the largest provider of incident response, at that time, we would get called by the media, anytime something was leaked, or a threat actor made a claim about a breach or data being sold on the dark web.

Now, we obviously could never talk about anything that we specifically did with our customers for confidentiality purposes, et cetera. So that was really what caused us to make the decision to basically bundle up all of the case data that we had anonymize it, of course, and then report out on the salient points. So it was always intended to be an external publication to address the concerns and questions over this growing area. Again, growing back in, you know, 15 years ago. We also saw, you know, the absence of factual data coming out at this time. And so being able to address misinformation with accurate actual data was important to us, so that we would be able to point organizations leveraging us into the right direction, right. And not just chasing what the latest headline was for root cause of the latest data breach.

03:59
Database decision, that's rare.

04:02
That's right. So yeah, sorry, I was

04:06
just thinking about my introduction to you and I, Business Information Security Officer, I'm sure people that are reading it going keep us I got that word confused. It's really, you know, chief information security officer to Cisco, right, John? No, it's not CES. So it's been so busy. So so just for the people think I screwed up most. Tell us what's your job and titles?

04:25
Absolutely. Yeah. No. So I am like you said the B. So for the Verizon business group. And you know, some companies use this be so setup, where essentially, I represent all things CISO to the Verizon business unit, I'm responsible for ensuring that our larger enterprise wide cybersecurity capabilities get embedded in the Verizon business group every day. In conversely, I'm responsive Row for ensuring that any of the unique needs for Verizon business group are then communicated back to the larger corporate information security team, and determine whether we can modify or introduce additional capabilities to address whatever the unique needs are. And if we cannot do that, then my team will provide that specific and unique service to the business unit. And just to take a pause. So we have the Verizon business group, which again is who I represent. And that's the unit where we provide big b2b connectivity and custom networking solutions, etc. And then we also have the Verizon consumer group, which most people are likely familiar with. And that is our, you know, cellular data plans, right? Your iPhones, consumer family plans, things of that nature.

06:00
I'm thinking of a data analogy here, but might work back before the football players had headsets on, they'd have something called a messenger guard, the guard would be sitting on the and they'd run it and say, play for and come back in. And so I'm insulting you, but you're like a messenger gardener. And she like you. You can you know, both sides, and you can convey information of what's going on in order to win the game. Exactly.

06:22

You got it. I love that. Oh, and a messenger.

06:24
Thanks a lot. Yeah. Nice. Thanks. You're gonna say after that. Okay, so we know that Verizon put together the report. So if we have this pain to get in broad strokes, if we look at the last 1015 years, what generally has happened over the last 50 years for your perspective. So it's

06:43
interesting, you know, and in fact, in this year as DVIR, there's a whole section dedicated to what's changed, and what has not changed. And so I think it's, it's important to probably just note that the DVIR talks in terms of the four A's, the four attributes of any incident, the actor, the action, the assets, and then the attribute. So for the most part, the actor has not changed back in 2008. External actor was the most common actor in breaches. And that remains true today as well. The when we talk about the actor that DVIR also looks at the motive, you know, why are these actor actors doing whatever it is that they're doing? And this is another area that has remained constant over time. So financial, right? Why are why are these threat actors attacking us? It's really for financial gain. Now, there's one interesting tidbit in this motive in that back in 2008, fun, the sort of ideological type of attacks made it into our charts, right? You kind of think about people doing this just to get back at someone, there's a grudge or they're just kind of in it to see if they can do it for fun or curiosity. And that really does not come into play today. Today, this hackers and threat actors, like I said, are really in it for the money. It's for financial gain. They're very organized, they're formal. And so I think that's a that's definitely a shift that we've seen over time. As far as the action, what the hackers or threat actors are doing, it's still hacking and malware. I think the biggest difference really, that that we see over the past 15 years is the asset, what is being compromised. So server remains the number one from 2008, still to today, but the big shift is that person, US people are actually the number two asset can be compromised. So I think that's, you know, that's a big takeaway, and should not be understated. For anyone who's looking to stand up right, or review an information security or a cybersecurity program, we have to really consider our people now, not just our technology assets.

09:39
I can remember years ago when when they talked about denial of service attacks, and now they talk about credential theft. So it's gotten personal, huh? Absolutely. Yeah.

09:48
And in fact, that's a great segue into you know, the what right the attribute which is the final ape, and back in 2008, and I can remember this to the payment card data, right credit card data was was kind of the the hot data if you will. And we were all scared, you know about having erroneous or fraudulent charges on our cards. Over time, if you're looking at the graphs in the DVIR, you can see that payment data has declined steadily over the past 15 years. And there are a lot of reasons why we have a lot of improved defenses in this area. You know, a lot of us probably listening are subject to PCI DSS which sets security standards around protecting this type of data. And the credit card companies themselves just have much more sophisticated methods of really identifying when attacks have occurred, and then can prevent, or at least mitigate future issues. But in the place of payment card data, to your point, the personal data, and specifically credentials, has

risen significantly over the past 15 years. And, you know, now, this is the kind of data that actually can be sold to other other threat actors, right, and be monetized and then effectively become the input to another breach. And that really, honestly, if you read the DVIR, and even, you know, kind of in a summary format, that's really the message of this year as DVIR is that the output of one breach is often the input to the next.

11:46
So what happens is a credential is compromised. And that leads to some kind of a phishing attack, and that compromises someone's credentials in the software chain. Is that kind of the flow?

12:01
Yes, yes, it can be so so generally speaking, the phishing attack will likely lead to the, you know, the the breach, right? So you know, you're kind of again, attacking the person to get in the door, and then able to steal the credentials or the personal information, which can then be sold to another threat actor, and then perpetuate Yes, the next, the next breach. So it's kind of that circle. And so the DVIR talks about how you can prevent that circle of a breach. Now, the other thing that we haven't hit onto and and I think we can go into it, too, is the fact that supply chain breaches or third party breaches are starting to have a much bigger role. And in fact, the DVIR believes that this could be a force multiplier for, you know, backdoor access, and potential monetization for these threat actors.

13:07
And in my humble opinion, what I see is that everyone's moving to the cloud authorization important, they're starting to automate things. Sometimes automation can unleash some of these supply chain attacks with with passwords, nothing else can be more and more difficult over the years, hasn't it become?

13:26
Absolutely, absolutely. There's, there's so many different, you know, threat vectors today. And so it's, it's really important to have your eyes on on all the different ways in,

13:39
I have to make sure that listeners go to verizon.com and download the report. That's right. And believe me, I saw a presentation Melissa gave, it was just it was, it was eye candy. It was like you have all these numbers, and someone makes it human accessible. It's like, you know, there's wheat in the field. And so it makes it bread. It's like they take all these charts and show you trends over time they isolate this, isolate that and there's so many, there's a whole section on the public sector you can take a look at. And so I think if you're just looking at how to present data, which is called Business Intelligence, maybe it's a study in that because it's Verizon put some money into this, haven't they?

14:16
Absolutely, yeah. And speaking of data, it's a significant amount of data that gets analyzed. So back when it started, it was about 500 cases that spanned a three year period. And again, this was all Verizon data, as we talked about, you know, how it all began. Now, over time, obviously, the reports grown, we have a total of 87

organizations now that share their data with Verizon. And this year alone, we analyze the DVIR is based on just under 24,000 security incidents and that includes about 50 to 100 actual breaches. with machine learning, artificial intelligence is leveraged to categorize and classify. And, you know, and plot the data with a variety of charts throughout the publication.

15:18
Now my lawyer friends, listening and maybe our technical people. So what did she say? Oh, a breach and incident? What's the difference there? I want a five hour answer on No. I mean, we have to because it's part of this report. So breach, so we have to define an incident in breach. Maybe you do that real quickly for our audience?

15:34
Yeah, no. So the DVIR uses a data schema that was also created by Verizon. And it's, it's called Varys, which stands for the vocabulary for event recording and incident sharing. Hmm. It's free. You can Google it and go out and check it out. So within Varus, an incident is defined as any compromise of confidentiality, integrity, or availability. And any breach in Varus is defined as the confirmed disclosure of information to an unauthorized party. So as I mentioned before, 5200 breaches 24,000 incidents, breaches are a subset of incidents.

16:21
So that's, that's the interesting part. I was just thinking about this graphical depiction. I interviewed Andrew Churchill from colliculi K in episode three, and go back to that, and they're trying to use data visualization. And maybe they're looking at Verizon going, Well, hey, Verizon managed to somehow present this data in a format that's acceptable. So from the perspective of a Federal Information Technology Professional, they can download the report. And they can get dazzled by all the charts and projections and everything else. But there seems to be some trends that are going up some trends going down. I think phishing and ransomware seem to be going up. What about the role of training and all this? You know, I mean, I've had, I've had people say that you can train a Harvard PhD and 4% of time they're gonna get allow a phishing attack. And other people say, well, at least it's not 20%. So So what about training? And?

17:17
No, I think so. So first of all, ransomware to your point going up, in fact, I believe the the factoid is that it grew Rose 13%. This year alone, which is more than the last five years combined. Combined, let's

17:36
repeat, combined.

17:38
Exactly. Right. Again, just reminder at its core ransomware is a method of monetizing an access. Right. And, and it's there's an interesting appendix in the DVIR. To that, that talks about this, and the authors did a ransomware economic study. So it's an interesting read, basically, you know, to summarize, they concluded that ransomware is not really like running a business, but more like playing the lottery. And until there's not a a

quick win on the other side, that ransom will, will continue to be with us. But definitely go ahead and check that that appendix out. Like I said, it's a good read. And then back to your question on training, John, you know, there, there's, there's obviously, a lot of technical controls and mitigating factors that companies can leverage to minimize their chances of being breached. But the human element is one that we really just haven't cracked yet. So the DVIR also has a changing behavior appendix that, you know, talks about, what are some of the things that we should be thinking about or doing when it comes to the human element? Right, there's no point of perfect mitigation. We're just too complex. But they do talk about training. So on average organizations, and this includes Verizon do about an hour of phishing training a year, you know, depending on your company, and again, what you have dealt with, you may need to do more. It also talks about phishing tests, what should they include? What should they not include? Do you need to have quizzes from time to time simulations of potential security incidents? And to be perfectly honest, the DVIR notes that we're still learning what works and what doesn't in the space? And, you know, that's okay. Right. That's how science works. We've got a we need to know what mitigations work and we're kind of working to get to two to that. So one of the things that that the DVIR does include in the changing behavior index is what you should expect in a test. That's meant to test what human element mitigations work, right? So what should you be looking for, to determine whether a test or quiz is actually meaningful or valuable. And it also lays out what you should expect to get in the results.

20:28
I'm just thinking about if I was, maybe this weekend, raking leaves talking to my neighbor, and they asked about Verizon, and there must be some perceptions that people get confused about this report. For example, they must think that oh, yeah, Verizon is trying to sell me their stuff. Well, no. Anything here, you know, in fact, it's free. Will Verizon just picked it up from like, the East Coast? No, no, it's a global amount of information. So it's, it's not it's used word scientific, it's an attempt to be at least as objective as possible. You know, it's, it's transparent. I mean, you talk about how you gather the data and use other organizations at other organizations. So there's some maybe there's some elements that people get confused about, those are the things that I think people have to read and reinforce that you're doing this for the benefit of the community, and you're putting a lot of money into it. And it's probably saving companies money in the long run.

21:17
You got it. And it's, it really is looked at and it's published to be a true research and thought leadership publication. It is not a sales tactic to your point. And, and again, as you noted, it is domestic and international. So the 87 contributors ranged from law enforcement agencies to forensic and law firms, different certs and the ISAC come councils and whatnot, that that share their data with Verizon.

21:51
And we talked about phishing, which, you know, I'm walking the dog and I get an email from Melissa and I opened and I get a trap that could happen. Not that's accusing you of anything. But you know, I think there's other human errors here, too. There's misconfiguration. Yeah, there's just someone told me about MFA fatigue, what's that? Yes, I'm getting bounced too many authorizations, approval, and all of a sudden they get in. So there's human aspect too, isn't it?

22:17

Yeah. Yeah. human aspect is attributed to 82% of all of the incidents and breaches reviewed this year,

22:27
humans, those darn humans got to get them off the system, don't we? Oh, crystal ball time, 15 years in the past 15 years in the future? How do you see the report changing in the next year? And what kind of challenges you have in putting together the next one?

22:41
Sure. Well, so I think that, you know, there is a plan to produce it next year, so everyone can mark their calendars and look forward to that it normally is published in the May timeframe. challenges, I think it all comes back to the data, right? When we talk about the fact that there's 80, plus contributors, these companies or organizations, they all have their own priorities, they all have their own resources and challenges. So it's not like everyone neatly submits their data on on a specific date. And then we have x number of weeks or months to analyze, right and go back and ask questions, it can be a lot of back and forth, to get the data to get the data in a format that is required. And again, because of the differences in time zones, domestic and internationally, it can be a bit chaotic, to pull it all together, and draw the appropriate conclusions, again, using those scientific methods that are also described at the beginning of the report. So that's, that's the main challenge.

23:57
verizon.com for the Deborah DVIR when I was doing my research this morning for this interview, I happened upon a phrase that I haven't seen before. And it talks about some people are targeted more than others. Maybe it's celebrities, maybe it's politicians, athletes, I don't know why they target an athlete, but they call it a very attracted people are very attracted person or some Is there a category for people to get attacked more than others?

24:25
Yes, I believe that is your you're talking about spearfishing,

24:31
maybe maybe very attractive, very attack people, some people really targets and that's the go after more than others.

24:36
Right? And then the for that the threat actor will do a lot of background and investigation and research online social media platforms. What does this person like? What are their hobbies? Where did they vacation, in order to really construct an elaborate scheme if you will, to get this person to, you know, buy and believe it and then ultimately Again, steal access credentials, or what have you.

25:04
In other words, let's say you're my neighbor, and you're at the beach and you email me and you go, Oh, I left the stove on in my oven or something, and and click on this to automate, bang, because the person would do

the research to find out more about the relationships people have, again, it goes back to the 82% of being human, doesn't it? Yes, it does. Wow. Yeah, I know that. So last few minutes here, maybe give our federal listeners some ideas of what's coming up. Next, more focus on edge edge computing, you know, people talk about stuff at the edge and more compute and more focus on maybe identity management, or where do you see the focus coming in next few years?

25:40
Yeah, I think identity management, asset management, for sure. Right. As everything becomes more, you know, virtualized management of kind of the basics, right. basic hygiene, I think is always going to be key when it comes to having a strong and solid cybersecurity program.

26:01
Back to the basics. That's right. That's right.

26:05
Any parting words before we leave, Melissa?

26:08
No, thank you so much for having me on. John, I think, you know, companies can use this DVR for multiple, multiple, in multiple ways, specifically to use use it to pressure test, an existing strategy, are you prioritizing is what you're prioritizing, relating to the key types of breaches and threat actors within the DVIR leverage it in production producing or, you know, approving business cases. So it really should help drive, like you said at the beginning data driven decisions. And the other thing too, is, I think it's important to not just read it once and be done with it, but continue to refer to it throughout the year, is everything you know, as you as you face changes in your landscape and environment, make sure that you're again, just leveraging this in any way you can

27:17
imagine if you're trying to make a decision about a vendor. And there's emphasis given to denial of service attacks, and maybe you personally think there should be more focused on credential. Maybe you can get the DVR and go Well, look, you know, this is what Verizon says about this. And they kind of bolster my case. And so there's an application of, of using it to persuade someone to make the correct decision that can impact everyone in this federal government. You got

27:43
it. And I think and the other. The other thing to note too, is within the pen axes, they have all different industries, as well as regions. So while there is the overall trends, and the overall message, it could be different for the specific injury. I know we're talking about federal, but if you're looking at a specific vendor, or again, you may be you're just you know, trying to help out one of your colleagues or a neighbor. There are very specific insights for the different industries that are also included. And those trends could differ from the overall. So check that out too.

28:25
That's good to know. Good to know. You've been listening to federal tech podcast with John Gilroy. I'd like to thank my guest, Melissa Gilbert, Executive Director, Business Information Security Officer at Verizon. Thank you, Melissa.

28:37
Thank you, John.