#232 – Inside The 2025 Verizon Data Breach Investigations Report

G Mark Hardy: [00:00:00] Hey, with all the excitement with RSAC and everything else this past few weeks, did you ever get a chance to read this year's Verizon Data Breach Investigations report? I did. I'm gonna share some observations with you right after this.

G Mark Hardy: Hello, and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader.

I'm your host, g Mark Cardian. Today we're gonna dive into the one of the industry's most anticipated publications, the 18th year of the Verizon Data Breach Investigations Report, DBIR, or 2025 DBIR to be more specific. And it's really a cornerstone report. We look forward to this thing. It's got a lot of information, a lot of data-driven insights if you want to go ahead and help make better decisions for your organization.

Also to see some of the patterns, the trends, and the [00:01:00] tactics that are shaping cyber crime as well as security issues. So today I'm gonna distill what I think are 10 critical takeaways for you. A CISO, a VP director, or aspiring to become a CISO. this information is for you, so let's settle in and, take a look at it.

First of all, you can go ahead and I'll put the link on the. And the URL on my website, so you can go ahead and download it for yourself. They do have a squeeze page where they ask you for your contact information, but once you get to the PDF page, there's not a squeeze page on that, so you can go download it as many times as you want.

I will, of course, respect their wishes to go ahead and capture your data. Your mileage may vary now as published on the 23rd of April, and it's 115 pages. Now, one of the things that I like about this, if you remember one of the, admonitions that was given by. Warren Buffett. He said, whenever you read an annual report, start with the footnotes.

Why would he say that? Because that's where they put the stuff that they gotta say, but they don't wanna say, in this case, I would say for fun, read the [00:02:00] 123 footnotes in the report. there's a lot of, I. Kind of cute stuff in there, including a reference to a customer complaint that is over 3,800 years old.

One that I just learned about today when I was looking it up. I didn't see a puzzle this year. I know in the past there have been puzzles associated with the report. Dave Schutz is a friend of mine, a gentleman I've known who was involved in the Schoo group that years ago. He kept winning all of my.

Contest. I used to do crypto contests for schmo, and this guy would win him each year at my grand prize, his round trip ticket to Vegas to go to Defcon. So I said, okay, I'm gonna teach you how to do it. And not only is he great at making puzzles, but he's great at solving 'em. So shout out to Dave if you're listening.

Anyway, let's take a quick look at the scope of this DBIR. This report looked at over 22,000 security incidents. Over 12,000 confirmed data breaches across 139 different countries. It's really a global snapshot of cyber crime as well as just mistakes that people make from a security perspective, but it's grounded in [00:03:00] data from the real world, and they look at their partners, law enforcement incident response teams, and a security executive.

You should know the value of actionable intelligence and the DBIR delivers just that. So let's take a look at 10 important elements for your strategic planning. Starting with a trend that I think is sounding alarms across boardrooms, number one, third party breaches is doubled to 30%. 30% of all breaches now involve a third party more than twice of what they had last year.

It's a real wake up call. If you're relying on vendors, partners, supply chains, if it's a software vulnerability and a third party platform, a compromised data custodian, these effects could be significant for you as a CISO, this underscores a need for robust vendor risk management. It's not enough to secure your own house.

It's great you got everything patched and you have all of the different, updates that are out there, but you gotta worry about your partners. As well. Now, what happens if they have [00:04:00] a report? Can you ask for a SOC two? Sure. Does that necessarily mean that today that they're not gonna be vulnerable? No.

So realize that a single week link in your supply chain can unravel years of security investments. So what you do for an action item enhance your third party risk assessments Mandate regular security audits have breach notification

clauses in your contracts. Your perimeter extends far beyond your firewall now, and you need to go ahead and manage that.

All right. How about number two, ransomware? it's been around and it refuses to retire. Ransomware, according to the DBIR report is present in 44% of confirmed breaches, up from 32% last year. Now if you're in the SMB space, a small, medium-sized business, it's even worse. 88% of those breaches that were reported involve ransomware.

The median ransom payment last year was $115,000 US [00:05:00] down from 150,000 the year before. So it's moving in that direction. It's a significant hit though, if you're an SMB, that's not round off error. That could be salaries for a few months for your people, and that's a big deal. Suggests that the, maybe vendors are, I'm sorry, not vendors, but victims are not willing to pay as much.

64% of the victims refuse to pay. Up from perhaps half of them two years ago. this means you got more resilience, probably better backups, better incident response plans. And remember, there's kind of two approaches of ransomware. There is the attack against availability on the CIA. Hey, oops, your files aren't encrypted.

Good solid backups. Being able to have a robust incident handling plan can help mitigate that. And more recently, we've seen attacks on confidentiality. oops, your files are encrypted. we don't care. We can restore them. Oh yeah, by the way, we've got copies of them and we're gonna [00:06:00] put 'em on payin. Or worse yet, we're gonna send them to the regulators and let 'em know that you're outta compliance.

so those problems are still there. But as an executive, what you need to do is prioritize endpoint protection and patch management. It's gonna go a long way to keep ransomware entry. Secondly, invest in offline backup so that those cannot be corrupted. At the same time, test your recovery. Regularly.

Don't just assume because it went one way, that it can come back the other way. I had an incident in one of my clients, or one of my executives fairly recently went ahead and got one of these new type of CAPTCHAs. he is not a technical person. Brilliant business person, great guy. But when this capcha, instead of saying identify the buses or the motorcycles, or click here till there aren't any traffic signals said, type A, Windows + R then a Control + V and Enter to prove you're a human. what's going on there? it had already, because you'd say run, click on this to [00:07:00] prove your capcha, you've copied something into the buffer. Windows R is a run, run command. Control V is a paste and then enter,

and off it goes. Running PowerShell scripts, making registry entries, trying to download malware, and essentially setting off all kinds of alarms.

we were able to block it. But the point was, is that could have been ransomware and the approach wasn't a weak endpoint, it wasn't a, unpatched system, it was an unpatched user. So as a result of that, we went ahead and we did an all hands training on that. So be aware of that. good defenses.

You can reduce the leverage on ransomware, but you really, I think you get the most leverage. By making your people suspicious and careful about what they do, and no fear in reporting a problem. And that's key. Why? Because if people are afraid they're gonna get in trouble, they're gonna try to hide it, it's gonna get worse.

It's gonna fester. If someone can pick up the phone and say, Hey, G Mark, I think I just did something stupid. Can you help me? Absolutely. And there's no [00:08:00] blame. There's no ha at the end, but rather it's let's work together and solve this. So try to create that culture. Okay, third takeaway ahead. exploitation of the vulnerabilities has surged 34%.

Now, I said that maybe your biggest attack vector is gonna be your people, but. 20% of initial attack vectors are now coming through exploited vulnerabilities, zero days in particular, because you really can't patch those because as a result, as we know, a definition of zero day is something where the attacker has found a vulnerability that the vendor has not yet issued a patch.

And so as a result, if you can go ahead and do that, so the MoveIt software breach, for example, which had havoc across education, finance, insurance sectors, kinda remind me of that. So there's a call to action on vulnerability management. How long does it take to patch? I remember when they first started talking about time to patch, it was like 354 days, and that was the old, report from Mandiant, and now it's down to [00:09:00] Patching Edge and VPNF floss to about 32 days. Still pretty good, but that's an awful big long window for someone to take advantage of you, and really only 54% of those vols are getting patched at all. That's a huge gap. So have a rigorous patch management program.

Prioritize your critical vulnerabilities. Use your CVSS scores. Nine point eights need to get fixed. Fives, nah, you can probably live with 'em And consider automated scanning tools. Stay ahead of the threat actors. Speed is important. You want to go ahead and beat your opponent to it. It's the OODA loop.

Observe, orient, decide, act. You wanna get inside the OODA loop of your attacker and you'll do better. How about number four, credential abuse. It's still a top threat. it, so attack vector, 22% of breaches if you have stolen or compromised credentials. hey, those are the keys to your kingdom, and the threat actors know it Now.

DBIR noted that 30% of the systems that were compromised by info Steelers were corporate devices. But 46% of those [00:10:00] were unmanaged devices that hold corporate credentials. Now, this is a real concern in hybrid work environments where your personal devices are gonna mingle with corporate device networks. depends on your BYOD policy and things like that.

54% of those victims had their domain show up in credential dumps, and 40% had email address credentials out there in data dumps. Now, as an security exec, you gotta double down on MFA across all systems. I gotta pull out my laptop here, get one of these things, get a UB key. In fact, get a whole bunch of 'em.

I'm not getting paid to push them, but absolutely. I find that having that type of a physical device token is going to be key. And of course, I just dropped my key fob, necklace into my water. Go figure. Anyway, cheers. But what we find then is that if you have MFA. It's gonna be a [00:11:00] lot more difficult for attacker to get through.

Yeah, I've seen some fairly sophisticated attacks that allow some workarounds, but in general, what you wanna be is you wanna be very hard to breach. You wanna make it such that the difficulty of getting into your system is so great that attacker's gonna say, it's just not even worth our time and energy to do it.

Also, look at credential monitoring tools out on the dark web. Now, I recommend you do not go ahead and start doing your own threat intel on the outside. Why? Because if you're poking around on the dark web and you get caught. I can come after you and say, Hey, we're gonna teach you a lesson. There are companies that do that for a living.

So let them go ahead and take on that risk. You can absolutely do threat hunting with inside your enterprise, with inside your network. 'cause you're expected to be doing that. And if that guy gets caught inside your network, it's Hey, it's part of the game. But don't go poking around out there.

And again, as I said before, train your employees. Make sure they recognize phishing attempts, which often will precede a credential theft. So assume your credentials may be compromised. If so, what would you do? Again, MFA,

[00:12:00] making it a lot more difficult. Even if someone had an ID and password, they're not gonna get in without that next step.

And also think about maybe geographically locking places down. I know you can do that in Microsoft Azure so that when someone tries to log in from a country that we do not do business with, that login should be denied right away. It also means, of course, you gotta coordinate with travel and HR when somebody is going over there that you don't inadvertently lock them out.

All right. Number five, espionage attacks. That is surged by 163% from the year before. Wow. That's now up to 17% of the reported incidents. Now, it's interesting that you look at the motivation, the espionage motivation. 89% of threat actors are still after financial gain. Alright, but 17% said, yeah, espionage too.

Now you can do both. This is why the numbers don't add up to a hundred. But this increase is a concern. It's particularly in manufacturing. Healthcare sectors are being hard. Hit nation state actors are targeting intellectual property sensitive data. [00:13:00] Web app attacks usually linked to espionage are up.

61% of those are driven. By espionage motives. And only 34% were motivated by financial gain, which I thought was interesting. Also, what do you do? Can you go ahead and interview the people who break into your stuff and say, by the way, what are you looking for? So I'm not sure how they get those numbers, but if you're a CISO in one of these industries, this is a red flag.

So harden your web apps with robust firewalls, intrusion detection systems. Make sure you got, web app fire also. compensate potentially for your developers who may not have the world's best coding or, trying to offload code to AI and things like that. Do regular pen testing. Identify your weaknesses and collaborate with legal and compliance teams to ensure that your sensitive data is identified.

So you know which one it is. And then you can also go ahead and make sure that it is in compliance, often encrypted at risk, encrypted in motion, and you limit the access to it. espionage, your high stake games. You can lose your company, you can lose, country. And so your [00:14:00] secrets are the prize and your part of the front line.

Number six system intrusions, in apac, so AsiaPac Pacific Region or apac, it's found out that if you're operating over there, if you have operations there, 83% of the breaches in the APAC stem from system intrusions up from 39%. Now,

that's huge and malware has been a key driver. According to the report, 83% of those incidents up from, 58% and more than half of those breaches involve well stolen credentials.

We just heard about that. So the surge highlights this region's vulnerability to external actors targeting critical infrastructure. Now, if you oversee APAC operations, prioritized network segmentation. Deploy advanced threat detection tools, and since ransomware was involved in more than half the breaches in the region, revisit your incident response plans to make sure they are tailored to regional risks.

If you're a global organization, you have to not only think globally, but think locally. Your APAC [00:15:00] defenses have to be as robust as those of your headquarters. Number seven BEC Business Email Compromise Losses soar. $6.3 billion in losses with a median loss of about $50,000 per incident. Now domestically, I, went ahead and I looked up the FBI's Internet Crime Complaint Center, the IC3, and that just came out recently as well.

I might do an episode on that. And that documented 2.77 billion in losses from 21,000 reports or over $129,000 each. So I guess it pays better if you're hacking Americans. Anyway, over 40% of these successful social engineering attacks today are BEC. Or Pretexting where an attacker is gonna impersonate an executive trying to trick an employee into transferring funds.

Now, unlike ransomware, the BEC incidents aren't gonna make headlines because most people don't wanna report them. They're embarrassed about it. But the financial impact could be huge. And as a security executive, you can [00:16:00] combat this by having strict verification processes for financial transactions.

I did a talk, as I mentioned, one of my clients had an executive who had, Done the Windows + R, Control + V, Enter. And so what we said is that look today with deep fakes and things such as that, you can get a call that looks and sounds exactly like your CEO, Hey, CFO, we're doing this sensitive deal. I need you to transfer money now.

Okay, great. unless you are doing it face to face, the concern is, this person having a deep fake. So what I recommend is to have the equivalent of a disposable secret. Probably if your CEO's on the road, he's not gonna call you five different times with five different deals in the same day. And so have something that you can agree upon that once it's been used, because it's a

possibility your communications channels are monitored, that doesn't work anymore.

And so work out some phrase, some exchange of information that you could go ahead and validate that. And it's, I'm busy, you gotta do this. Oh, I forgot. Or whatever. I'm sorry. That's a red flag. [00:17:00] And. If you wanna see the real extreme of that, go look up the old black and white movie Fail Safe from the early 1960s and, lemme know how that goes for you if you haven't seen that before.

But help your employee spot red flags and usual email or domains urgent payment requests and email security solution. You can flag impersonation attempts I have in my Microsoft account there for exchange, you can do security rules and one of the things I do is have impersonation blocking. So if a person says that they're one of these key executives and it's not coming from. A known place. if I know the CEO has a Gmail account, I'll put that as an exception. But if it's, Mr. Big at Yandex au and it matches Mr. Big as my internal person, it's gonna get rejected. It's not even gonna get delivered. In fact, I delude deliver it. I deliver it to myself. It's a CISO and a special thing. Let me examine it to see if it's a [00:18:00] indication of higher risk. It's much of a human problems as a technical one, but your people need to be your first line of defense.

Number eight, your human risk persists, and the DBIR reports about 60% of your breaches involve a human element. Error. Phishing victims mis configs, so they make a mistake, a slight drop from last year. But don't let it fool you. If you read the footnotes. They said there's a lot of fun. The footnotes. It's almost as much fun as the Monty Python, the Holy Grail subtitles, number 35 says they've been, they reclassified some of last year's ransomware breaches from extortion, which is social to humans.

So it really didn't drop, they just changed the, they moved the goalposts a little. But humans remain your greatest vulnerability. As well as your greatest asset. Now, for a CISO, this means you have to invest in security awareness training that's engaging and role specific. The generic one size fits all isn't gonna work anymore.

Simulate phishing attacks to test employee readiness, but again, create an environment of no fear. Don't have a wall of shame. Don't go ahead and [00:19:00] score eight people who screw up because they're gonna not trust anything that comes from it. Security, and then don't overlook mis configs. Remember, regular audits of cloud environments can catch an error before they become a breach.

The DBIR reminds us technology is only as strong as the people behind it. Number nine, industry specific trends demand attention. Our ninth element is the DBIR focus on these industry trends. Manufacturing and healthcare are facing, as we said before, rising espionage attacks. Education, financial and retail sectors are dealing with things like ransomware and credential abuse.

SMBs, regardless of the industry, are disproportionately hit by ransomware with about 88% of the reported breaches involving this threat. And that may not be because 88% of small businesses get reported, but it might be the only thing they bother to report. As a security exec, tailor your defenses to your industry risk profile.

if you're in healthcare, prioritize patient data encryption. If you're in retail, focus on securing your e-commerce platforms. These industry breakdowns are [00:20:00] very valuable, using to benchmark your defenses against your peers and anticipate some of your threats. Number 10, the DBIR points to a need of multi-layered defense strategy.

With these third party breaches, ransomware, espionage, human errors on the rise, there's no single solution's gonna work. So this report emphasizes taking proactive measures, do patch management. Should be doing that, right? MFA, do that employee training, do that. Network segmentation, vendor oversight. This means you gotta align your security program with your business objectives by the way you're doing that.

It's a little bit easier to get funding as the CISO too, because you can point to a business value instead of you just being a cost center, engage your board. Secure budget for advanced tools like AI driven threat detection. I have a culture of security where everybody feels responsible. And Chris Novak, who's Verizon's VP of Global Cybersecurity Solution, says that DBIR IR's [00:21:00] findings underscore the importance of a multi-layered defense strategy I mandate.

And this ferone I'll decided our top 10. I'll do number 11. A data leakage to Gen ai. Yeah, you're wondering where that is. So it's a new and rapidly emerging concern. It's on pages 24 and 25 in the report, and it notes a significant uptick in incidents where it's sensitive data, like proprietary code, customer information, internal documents have been.

Inadvertently exposed through employee interaction with Gen AI tools. 12% of the data compromise incidents in this past year that were reported involve employees inputting sensitive information into public or insufficiently secured

AI platforms. Oops. It's a 200% increase from last year. it's mostly 'cause people are now figuring out it's, Hey, I can do stuff with this.

And so it's really alarming in industries like technology and finance where intellectual property and client data are gonna be. Prime targets. Now many employees are unaware of the risks. They'll use AI tools for tasks like drafting an email analyzing data. They don't realize that [00:22:00] these platforms can store share inputs externally.

and so it talks about things such as, hey, which is bigger, 9.9 or nine point 11, and then you end up getting some other corporate information leaked with that. Or how many RS in strawberry? I dunno if they fixed that yet. I'll have to take a look. But, establish cure clearest policy on AI tool usage.

Specify which platforms are approved and require data and anonymization. Lemme say that again. Anonymization that sounded better. Before input. Try that fast Five times. What do I mean by that? It means that if I'm gonna go ahead, I'm gonna set a letter to, client X and I'm gonna talk about system y. I wanna go ahead and substitute something in there.

It's gonna say Bill instead of Joe. It's gonna say, Big instead of small, whatever the idea is, that you tokenize it, let it do its thing. If somebody grabbed the tokenized word and it's full of code words, they're not gonna really figure out what you're talking about. They'll figure out, what you're talking about, but not for whom.

And I'm pretty sure that there's some tools out there when I was [00:23:00] over there at RSAC that I just didn't catch, as I mentioned, last week, I had to come back early. by the way, my little dog is here on the floor with her laying on her back and she's healing up nicely. So if anybody's worried about the fate of my little Pomeranian, she's doing okay.

but also, Think about data loss prevention, DLP solutions. You wanna block sensitive data from going out to an unvetted AI systems. Now it turns out that if you don't pay for your ai, you're not paying for the product, you're the product. if you look at, for example, Microsoft Copilot, they have a deal in there that actually pay them some money.

They will agree that they will not train on your data. It stays local to you. And of course, if you've got enough processing power. Download a LAMA or do something like that and do your own AI models locally. But also, again, it comes down to training programs, helping people know they use that. It's,

there's a great allure in that it says, Hey, I can just throw my work at Gen AI and all my homework's done and I can sit around and play with my dog all afternoon.

it's really also for you as a leader and a manager, something you gotta look for. Now, [00:24:00] I had a gentleman work for me going on. Couple years ago now I remember the day he discovered GenAI. All of a sudden his responses went from yes or no, or I'm on it to whereas it is critical to share this information with your subordinates.

It's important to understand the overall. And it's no, he doesn't write like that. Where in the world this stuff come from. And once I figured it out, it's stop it now. Eventually it's gonna get good enough that you're not gonna be able to tell the difference. But for right now, I think I can.

There we go. If you're watching on video, here's my little doggy, she's back up here to say hello, which is fine 'cause we're pretty much at the end. So be careful that your AI doesn't become a Pandora's box and have problems. So this DBIR report isn't just a report. It's a mirror. It reflects us back as what we're doing, our challenges and our opportunities.

Cyber crimes evolving, nation state attacks are involving, but so do our events as they need to evolve as well. So as security [00:25:00] executives, you're the architects of resilience. Use these elements to guide your strategy, tackle your third party risk. Fortify against ransomware. Patch your v quickly protect your credentials.

Go ahead and come up with defenses against espionage. If you're running an apac, have better defenses out there. Combat your business email compromise. Train your people, tailor to your industry. Build layer defenses and, limit what your people can put on AI without knowing what it is. For you. This is a daunting threat landscape, but if you have data-driven insights like the DBIR, you're not fighting blind.

So thank you very much for listening to this week's episode of CISO Tradecraft. If you found it valuable, share with your peers. Go ahead and subscribe. We're on, LinkedIn. Also, if you're not following us on LinkedIn, we have a lot more than just podcast. We also have a substack newsletter, which is a summary of this, so you don't have to listen to me talk the whole time.

You can read it on a plane or whatever. Also, if you wanna download the full DBIR report, you go to verizon.com slant business. [00:26:00] Slant resources.

And of course as they say, they'll direct you after you give 'em their capture information to a PDF page where you can do that. But meanwhile, I think it's well worth your time to take some time reading it and, you gotta look good insights.

And again, have fun with the footnotes and if they still have a puzzle there, somebody let me know. 'cause I don't know if they still do that anymore. Anyway, this is your host, G Mark Hardy. I appreciate your time. thank you. Until next time, stay safe out there.