|  |  |
| --- | --- |
| Joe Dora: | Hey everyone, I'm Joe Doria. |
| Daniel Newman: | And I'm Danial Newman. And we are the Main Scoop- |
| Joe Dora: | The Main Scoop. |
| Daniel Newman: | We've done the Main Scoop now for 10 episodes Joe, and it's been a lot of fun. But one thing we haven't done before is tape the show in front of four, five, 600- |
| Joe Dora: | 600 |
| Daniel Newman: | ... Of your closest friends. And soon to be mine. |
| Joe Dora: | Absolutely. It's great to be with you guys today. And we have a great guest today. |
| Daniel Newman: | Joe, I'm thinking though, you got this cool t-shirt... By the way I would never wear this on my own. |
| Joe Dora: | He made me do it. |
| Daniel Newman: | What do you think? You like it? The Main Scoop? Everybody want one. Yeah? Joe lets welcome Joe. All right. So, a lot of you are probably wondering what is the Main Scoop. |
| Joe Dora: | What is the Main Scoop. We have a little something for you to tell that story. |
| Daniel Newman: | Roll it. |
| Speaker 3: | One, two and three. |
| Daniel Newman: | All right everybody. Help me out here. Does it look better here, or right here? All right. Clap us in. Three, two... Come on guys. Do it again. Three, two, one. |
| Joe Dora: | Hey everyone, welcome to the Main Scoop. I'm Joe Doria. |
| Daniel Newman: | Daniel Newman |
| Joe Dora: | We have a great guest coming out. I think today when you get to meet and learn about our guests, today's all about cybersecurity. |
| Daniel Newman: | Absolutely. We're here at the Share Conference. We're in beautiful Atlanta. We've had some really prolific guests, as you've seen. By the way, anyone has been on the show in the audience. Hands. All right, I see a couple. Applause for the former Scoopers. By the way, everybody out there that's listening to this, because this is a podcast as well, you're like, "Who are you talking to?" This show was being recorded in front of a live audience. Yes. Joe, this is different though. By the way, this guy's different. He doesn't look like Greg Latko, does he? Now, is that good or bad? Anybody want to take that chance? All right. Joe's not going to respond to me. |
| Joe Dora: | We do miss Greg. Greg wishes he could be here. Of the 10 Scoop productions we've done, I've done several already with this guy, but Greg has done more of them. He wishes he could be here at Share but is unable to be here this week. |
| Daniel Newman: | I believe he sent us a wish; he sent me a text right before we started. He said, "Dan, break a leg." All right, so security. Let's talk about security. |

|  |  |
| --- | --- |
| Joe Dora: | Talk about security. |
|  | The other day you told me the story and I said to you, Joe, we need to tell this story in front of the audience at Share because it really sets up the stage really nicely for what we're going to talk about when our guest comes out here in just a moment. |
| Joe Dora: | Yeah. I call this a warmup. It's a warmup and it's basically what's going on with cyber-attacks. In this particular case, that I'm going to refer to as a phishing episode, a colleague of mine, friend of mine, fell victim, fell prey on the mobile phone, click the link. Everyone in this room knows what's going on with that type of situation. Hopefully, you recognize it and you don't click that link. In this case, she did. Pretty much as soon as she was done with it knew like I'm in trouble here. Called her bank, had her credit card canceled Safe. Safe. I handled it almost within 10 minutes. The sophistication of the scammers is getting just bigger and bigger.  What they did was they knew she was going for a replacement card two days later and called her back and said basically, "Hey. We want to secure your card today. We know that you had this situation play out." Of course, the second trap was set, and she fell prey again. The net of that was they did cash advances out of her credit card into her checking account and withdrew like $8,000 from our checking account. I heard that story and I was like, "Wow. This level of sophistication is really going to the next level." That's the consumer side of it, of course. |
| Daniel Newman: | I think these stories are all microcosms of the reality of today. Every one of us has probably gotten a data breach alert now. Sometimes you get these alerts and you're like, "Do I do anything with this? Should I act? Why is my password my children's name and then 1, 2, 3, 4." Something like that. Maybe it's time to grow up and use a real password. Then you heard just this last week, I think it was Last Pass or Pass Pack ended up getting hacked. You have some of these sophisticated tools that are supposed to be the ones that prevent us by having randomly generated passwords. These are just personal consumer things. Of course, everybody in this room though has got to be thinking bigger than that. We've seen security move from a consumer conversation to a board level conversation.  I think three, four years ago as an analyst, I looked at the market and I said it always felt like companies were spending on security the exact amount that was at this line between risk and cost savings and reward. What I mean is what's the least we could possibly spend to make sure our environment is secure, where, if we do get breached, we have all this leftover capital. Now, it's at the point where I think the damage that gets done when we allow our company to be breached ... By the way, these breaches can sit inside companies for months or years before they even get discovered. The risk is massive. Companies need to get out in front of this.  I think, Joe, you and I know a little bit about this stuff, but I think this would be the perfect time to introduce our guest. |
| Joe Dora: | Yes. Our guest is Mark Wilson. Mark, come out and join us. |
| Daniel Newman: | Good to have you. |
| Joe Dora: | Mark, 40 years, actually 43 years as a mainframer, which is amazing. I've been in the mainframe business and a mainframer myself for 15 years, which gives me rookie status in this room. 43 years and you're the only mainframer I know who started his career at age 16. If I could just take a second and do a shout-out, we have somebody else in the audience who is out there. Enzo, I don't know if you could just wave your hand. Hey. There you are. This young guy is a senior in high school and just a shout-out that he has a Z14 in his home and started in eighth grade. He outdid you. |
| Daniel Newman: | Totally normal. |
| Joe Dora: | 14 versus 16, but 43 years all in the mainframe space. You're an ethical hacker. You're the founder and director of a firm, Vertali. Welcome. |
| Mark Wilson: | Thank you. |
| Daniel Newman: | Why don't you give us just a little bit more on the background, the work, kind of what led you to here, why you've stayed in the mainframe space? I think everybody would be interested in kind of what's the hook. |
| Mark Wilson: | The hook for me was the technology, as a 16-year-old. As I sat in front of that green screen, and it was this is a piece of code. I was interested from day one and had some really good teachers and mentors. Then as you gain experience and you start seeing what this technology does for the world today and what we can do with, it was just a no-brainer. I was in all the way. I think if you split me down the middle it would say mainframer or security or hacker, but mainframer. |
| Daniel Newman: | Seems to be deep in your heart. |
|  | Very deep in my heart. Some folks out there will know that I did a little Valentine's Day post on LinkedIn and my love affair with the mainframe almost 43 years. Yeah. Very deep, very passionate about it. Always have been. I think today we have a responsibility to bring through the next wave of mainframe technicians, mainframe developers, but we're also custodians of that platform and making sure it's secure. People think it's a mainframe, it's secure, and it's securable. We have work to do. Some people do, some people don't. I'm very passionate about it. |
| Joe Dora: | On that comment, I have a question for you. Start at a broader level here. I know you've been in the market for 43 years, but let's take the last 10. Can you give me a guesstimate of the percentage of enterprises that you know are doing it right, they're on their front foot and governance and security and tools and all those things are being applied to avoid the risk that Daniel was talking about. What percentage are on the front foot? Then what percentage, over those 10 years, would you say is on their back foot, maybe has more to do and they're not getting themselves in a position to prevent or get past the bad scenarios? |

|  |  |
| --- | --- |
| Mark Wilson: | Yeah. Good question. Today, I'd probably say about 25% of the clients we talk to are on that front foot. My mission and what we do, day to day, is to move that 75% into that 25 and make it 100% on that front foot. About 25% of them do it, as we would say, correctly, rightly. |
| Joe Dora: | Even there, if you're doing it right there, there's the sophistication that we were on earlier. You're going to potentially have to still deal with these kinds of problems. But I think that's interesting to me that 25% are out in front, meaning they're really doing it right. That's aspirational, I think, for the other 75%. |
| Mark Wilson: | Yeah. Absolutely. I think, you look at how sophisticated and how motivated the bad actors are. It's a business. It's a multi-billion-dollar business. This is not the kiddy in the bedroom with his pizza and his full fat coke and his baseball cap on the wrong way around, sat there, trying to hack a mainframe. These are businesspeople that have org structures and help desks. You suffer a ransomware attack; I get a better response when I phone somebody like that than I do off my mobile telephone company. Yeah. They answer the phone quicker because they want your money. Yeah. That's quite scary. Yeah, |
| Daniel Newman | They seem to have the ability to genuinely, like your friend, went through, make intelligent people, capable and competent people believe in the scam. By the way, this is happening now at enterprises. I'm really interested ... |
| Daniel Newman | And by the way, this is happening now at enterprises. And so, I'm really interested, Mark, you mentioned the 25%, what is the ethos, the DNA, of those companies that you're finding? What are the questions that they're asking you about their transformation to enable that they're on the right path? Because it's not just about threat detection. It's not just about securing your perimeter anymore. You have to be asking better questions because these things are happening from the inside. These folks are very creative. |
| Mark Wilson: | They're breaking in. It's not just I have good antivirus on all of our edge devices anymore.  Yeah. For me, most of it, it's about the attitude from the board, yeah. And it's, yeah, how they see the platform in their digital journey, whether we call it the digital background or the transformation. But it's they see the importance of it, and therefore they can align risk to it.  So we talk about risk. We don't talk about APF libraries and link lists and SVCs. We talk about risk. And what we've learned over the years is we have to talk the C-suite language and explain everything to risk. And when they understand the risk to their business, then you can have a conversation about how you invest in it, what you do, what's the right thing to do, and investing in people, investing in tools. Yeah. But everybody's totally different, so you need a slightly different process for everybody, but taking all that technology and deploying it properly. |
| Daniel Newman | So, a hypothesis, you can't complete your digital transformation without a security transformation. So, the boardroom all understands digital transformation, but I would argue that a lot of the boardrooms do not truly understand security transformation. How do you get it through to the board to understand you can't complete a digital transformation without completing a security transformation? |
| Mark Wilson: | I mean for me, coming from the technical side of it, it's using the right language and talking to them as risk and what this can do to the business. But educating the senior managers who have to upsell to their directors, to their C levels to get them to talk the right language. And we are seeing, and in that 25% we see, yeah, the CISO sat at the board meeting. We see the guy who owns security operations sat around the table when they make business decisions about investment, about people. Yeah. |
| Joe Dora: | I think, too, the technology is there. You have to get the ethos right and the right conversation with the board, but the technology is there to ... if you get on your front foot, to the earlier conversation, and use the technology to help protect your business. |
| Mark Wilson: | I mean, the most frustrating thing for me is sitting with a client, and they've got all this technology and they say, "Can you come and do a mainframe penetration test?" And we do the test, and they're generally successful. And we say, "All this technology you've got, if you'd have deployed it, you would've thwarted us. You would've noticed what we were doing." And it's there and it's paid for. They just need somebody to encourage them to go and deploy it and use it. Because we've got great technology from what Broadcom do, with what IBM do and all the other vendors. Yeah, there's a mass of tools out there. Just go use them. |
| Joe Dora: | That's right. Yeah. |
| Daniel Newman: | I'm glad you said the M word. You what the M word is? |
| Joe Doria: | Mainframe? |
| Daniel Newman: | God, you're so good. I don't think we ever need Greg back. |
| Joe Doria: | Come on, Greg. He knows Greg's going to watch this. So, he is just ... |
| Daniel Newman: | We're just having fun. |
| Joe Doria: | Yeah, we're just having fun. |
| Daniel Newman: | But you said the M word. And when it comes to mainframe and innovation, I've been one of the analysts. I'm not from the ... I don't proclaim to be from the mainframe world. I come from a broader IT viewpoint. And I look at public cloud, and I look at the hybrid. And of course, I'm an advocate for the mainframe and the role that it plays, but I've published, in many cases, that there's a gross overstatement of how mature we really are in the mainframe cycle. And in fact, the mainframe, in my opinion, is going to continue to grow and continue to be critical to businesses being able to successfully innovate. So, there's this intersection of security, of transformation, of innovation that all happen and start on the mainframe.  As you sort of bring those two, three things together, how do you talk about the mainframe, specifically as a mainframer? Love mainframes more than West Bromwich Albion. Is that true? |
| Mark Wilson: | No. |
| Daniel Newman: | Okay, close. |
| Mark Wilson: | Close, yeah. |
| Daniel Newman: | Someone that genuinely has been from this space for a long time, and you talk about it with people who probably are cloud believers, pure purists, we don't need ... How are you keeping them seeing the opportunities for innovation on the mainframe? |
| Mark Wilson: | Try to take the blinkers off them and understand that it's just another server. It's just another computer that has a set of special capabilities, and use the capabilities, whether it be for transactional throughput, whether it be for security. Yeah? But take the blinkers off. It's not just ... Yeah, it's not a mainframe. It's a big server that has a unique set of capabilities ... and integrate it. I hate going and talking to people and they say, "We've done an identity and access management rollout." And we go, "And what about the mainframe?" "No." "Why not?" "We don't understand it. It's too complicated." It's not. It's another computer, yeah? And it's trying to educate people that we can do these things, we can integrate the mainframe, we can secure it. It's just they've got to want to. |
| Joe Dora: | So another moment last week for me, opening up my newsfeed, I saw from your area of the world a customer, a big enterprise insurance company, that took a bad breach there. And you know what struck me was the breach happened in 2019, and they were first week of March of 2023, they're talking about what the GDPR finds were. And as the marketing role that I'm in, I think about customer experience and trust and how do you keep that?  And they found out about this three and a half years ago and reported it actually, which is the right thing to do. Now they've sort of been suffering through three and a half years, and finally are now at the point where it's coming back out with the fines being promoted out there.  So, I think inside of that story though, and we haven't touched on it yet, is obviously, and I think we would be remiss not to talk about it, is the regulatory mandates that you have to keep pace with and then complying with them. So, what's the compliance strategy that you talk to customers about when you're talking about this situation? |

|  |  |
| --- | --- |
| Mark Wilson: | I mean, most of it comes down to understanding. So, in Europe at the moment, we've got what they call the DORA Act, Digital Operations and Resiliency Act. That's not here in North America yet, but if we've got it in Europe, it's something's going to happen here. And it's understanding what that means to you as an organization, so you can start thinking about how you comply. Do I need ... Is it hardware? Is it technology? Is it people? Is it process? But staying on top of the constant changing world.  But they're kind of, Sarbanes-Oxley, they're all now SOX and GDPR and PCI. They're just normal things we deal with. Yeah? DORA will be the same. But it's just staying ahead of it and staying on top of it. But you need to understand it, need to understand every ... impacts the business. And then how can the technology help me be compliant? It won't be a single solution. It'll be, "I need a little bit of that and a little bit of that and put it together," and then that's how you stay on top of it. |
| Daniel Newman: | So, you mentioned this insurance breach, three-plus years, data's being potentially taken out of the company. A lot of times, even once they identify a breach, that doesn't mean they're immediately able to stop the breach or able to remove it. We've seen cases where these particular ... These data leaks can go on for months and years. And as you mentioned, they found out, reported it, and it's been multiple years, and they're still dealing with the potential fallout with their customers.  And that might be an interesting question, Mark, is ... You mentioned the special capabilities of the mainframe. And that's been one of the big reasons why as an analyst I've stayed on as a believer, is not only compliance and governance, but truly, genuinely, the security and the ability to lock down the mainframe for highly regulated industries just makes a lot of sense, things that the public cloud have not been able to truly accomplish. But you probably have clients that have been hacked, and they have been breached. |
| Mark Wilson: | Yeah. |
| Daniel Newman: | How do you help them come back from that? Because that, to me, is the biggest question is, "You didn't do enough upfront. Or even if you think you did, once you're breached, you're breached." How did they come back? What do you recommend to them? |

|  |  |
| --- | --- |
| Mark Wilson: | Well, this comes back to what Joe said about this three, three-and-a-half-year gap. So, they had the breach. They reported it. And then the regulators spent three and a half years talking to them to understand how well they had tried to protect themselves. Because the scale of the fine is predicated on how much work you did. We won't stop them. Okay? We won't stop them. We need more of the 75% joining the 25%, but we won't stop them. It's a conversation because there's so many different things you can do. We had one in Europe a good few years ago-  We had one in Europe a good few years ago now, where the guy was an insider, he went rogue. And I sit down, had a conversation with the security people and I said to them, "When you onboarded this individual, did you do all the background checks on him?" They said, "Yes." I said, "How long has he been at this establishment?" "25 years." Now, a lot can change in 25 years. Now, this guy had been divorced twice and developed a gambling habit. Now, that was part of the reason he went rogue because he needed to do that.  It's simple things. Well, why don't we reassess our staff every two, three years? It's little tweaks in the processes. We talk about the bad actors taking the data today and just storing it because we can't break... If it's encrypted, we can't break the security on it, but we might be able to in two years’ time or three years’ time. And so, they harvest the data, then sit on it, then use it. So, it's trying to explain to the clients how this happens, why it happens, and what defenses they can put in place to protect themselves. But it's no one simple answer. |
| Joe Dora: | That's story for me, just talks to the zero-trust architecture. 25-year employee, but zero trust. That's not just for the ones outside of your company, the ones inside as well. |
| Daniel Newman: | You definitely have that trend line, and I know people that are against the zero-trust framework, but I think largely it's proven that you're a little bit better off being too safe than the risk of being undone and being sorry. Now, I want to pivot because as we talk, I want to... As we wrap up, I want to talk about what these companies can do, of course, depending on where you are in the ecosystem, how you either work with your clients, how you develop your next generation of software, but investment. One topic though that while it's not specifically just about mainframe but has been part of the mainframe has been AI. And over the last few weeks with ChatGPT, OpenAI, Salesforce came out with theirs today, Salesforce GPT, but the rapid onset of generative of large language models, obviously, the mainframe space is going to have to capitalize on the power of AI. How much can AI enable the future mainframe? And of course, how much can AI enable a more secure environment in mainframe? |

|  |  |
| --- | --- |
| Mark Wilson: | I think it can impact it massively because one of the reasons people fear the mainframe is the amount of data that we hold, but also the amount of data we can generate. So, you think about what we could do by way of logging data and sending it to one of them, those CM tools, Splunk, QRadar, doesn't matter what it is. And we say we can't actually ingest that data and process it. Keep the data on the mainframes and start running those AI and ML models against it to try and do that predictive analysis, what's happened, behavioral analysis. What's the normal pattern for Joe when he logs on Monday through Friday? All of a sudden, we're seeing a log on a Saturday morning and he's doing something slightly different.  So, we can get very much on the front foot here and use the power of the technology to protect ourselves. And I think that's going to be a massive space for mainframe security, how we harness that technology and leverage all the data we've got because we have the data. There tends to be a lot of it, and that's a big problem, but we can solve it. |
| Joe Dora: | Definitely. I agree with that completely because for the ecosystem and for all the players in this space, everyone's looking at AI technologies and machine learning and applying it to not only cybersecurity opportunities, but performance management, different DevOps, all the different areas that touch in our critical to the mainframe vitality in the enterprise. So, I agree with you on that. |
| Daniel Newman: | So, I have one more question, Mark, and then I'll let you go eat. It looks like everybody's enjoying their lunch, but at least the clinging has stopped. So, everybody's done eating and now they're being forced to listen to you. So, getting the investment level right for security, I've started with this topic and I want to end here. I think over the last few years, boards have increasingly looked at spend. And I know when I sat down with Arvind Krishna, he said to me, "The most protected line item in any company's budget right now, even in this difficult market, is going to be the IT line item." And I would say even furthermore, it's specific line items within IT that's going to obviously include core business applications and security.  How does a company know that they're investing the right amount in security? It's harder with security than other things. It's harder to know than if you have enough licenses of an application or if you have enough storage for your data. Security is something you can always fortify. It's the three wolves, it's the straw house, it's the whatever, it's the brick house, it's the stone house, it's the steel. How do you build that fortified house but not spend too much? How do you help companies do that? |

|  |  |
| --- | --- |
| Mark Wilson: | And for me, it's testing and testing and testing. And you might do that with tools, you might do that with an internal red pen testing team, it might be an external team, but you have to keep testing the controls and you have to constantly test all the controls. You can't say, "I've done a pen test on a Monday, and I'll come back and look at it in six months’ time," because the bad actors will know what's going on. They're probably most likely already in the organization, in the network. So, you have to constantly, constantly test.  And that's when we start talking about automation. How can we automate this? We've got tools, we've got mainframe automation tools, we've got things like Ansible and all that stuff, but constantly, constantly testing. You have to test the controls and constantly review them. And if you get a negative result, how do we fix it? Do we need to change a process? Don't test it, fail, and then test it and fail again. Go and fix the root cause. Is it a process? Is it a piece of technology that we need to upgrade, change? But you have to constantly test it. |
| Daniel Newman: | Let me ask you a trick question. I'm giving you time to think. So as long as you- |
| Mark Wilson: | [inaudible 00:36:56] question first. |
| Daniel Newman: | Yeah, it's a trick question. It's not really a trick. Maybe it's a trick. Let's see how good your answer is. When you know what you're testing for, it's pretty easy to do the testing. It's not easy, but it's easier. But with this level of sophistication, and it is a bit of a... It's a tortoise and a hare of black hat sophistication, white hat catches up, we patch it, we fix it, we protect it, and then they figure out a new way. It's cat and mouse. How do you know that you're testing for all the right things? |
| Mark Wilson: | You don't. |
| Daniel Newman: | Good answer. |
| Mark Wilson: | You don't know you're testing for- |
| Daniel Newman: | No, I'm actually really glad you said that. |
|  | But what you've got to do is take the behavioral data and understand what's going on the system 24/7, 365, and use that to look at that, look at the emerging threats, talk to the risk and compliance team, talk to the wider security teams in the organization and collaborate. So, we are seeing a new emerging threat. Okay, do we need to build some tests? Is it applicable to the mainframe? It might not be, but if it is, what do we do? This is why we need your 24/7 security operations centers need to understand what's going on the mainframe. Mainframes exclude, we don't understand it. People call it, non-mainframers, call it the evil mainframe, and it's only evil because they don't understand it. They put it in a corner and say, "No, don't understand it, don't use it. Can't protect it." Yes, you can. |
| Joe Doria: | I think that's a good way to get to the close of our session here. And all you just said to me is all that front foot actions that people can think about and bring into their to their business. |
| Daniel Newman: | I think the sound bite is, the mainframe is not evil. You can protect it. Mark Wilson, the main scoop. |
| Joe Doria: | The main scoop. |
| Daniel Newman: | Mark, thank you so much for joining us. |
| Mark Wilson: | Thank you. |
| Daniel Newman: | We really appreciate you joining. Joe, good job subbing in for Greg. Greg, we miss you buddy. And to all of you out here in this live audience, this first time doing the main scoop live, thank you so much for joining us, thank you so much for eating with us, and have a great rest of your share. |
| Mark Wilson: | Thanks. [inaudible 00:39:25]. |
| Daniel Newman: | Thanks. Good job. |
| Joe Doria: | Thank you. |
| Mark Wilson: | Thank you. Can we walk off then? |
| Daniel Newman: | [inaudible 00:39:29] back. |
| Speaker 4: | Stick around. We have some trivia coming up, and we do have prizes. There's also a lot of [inaudible 00:39:36]. |
| Mark Wilson: | Watch those steps. |
| Daniel Newman: | Good job. Good job, boys. That was fun, huh? |
| Joe Doria: | Good job. |
| Mark Wilson: | Thank you. |
| Daniel Newman: | Thanks. That was good. |
| Mark Wilson: | Thank you very much. |
| Daniel Newman: | You were awesome. |
| Mark Wilson: | Thank you. |
| Joe Doria: | Wasn't I awesome? |
| Daniel Newman: | Yeah, of course. |