Daniel Newman: Hey, everyone. Welcome back. We're here at the The Six Five Summit, and in this next session I'm going to be talking to Greg Lotko, SVP and GM of Broadcom's Mainframe Software Division. We're going to be talking about navigating rough waters with the captain. Or is he? Greg Lotko, welcome to The Six Five Summit.

Greg Lotko: Delighted to be here, Daniel.

Daniel Newman: Yeah, it's very exciting. I've wanted you here for a few years. I've been following the Broadcom Mainframe Software Division, and really glad you're here. So captain, my captain, the theme of this event is really about navigating rough waters. And of course we set the theme of this early in the year. And I think we were on the right track after a few years of rapid growth, we've hit a period of austerity. We've hit a period where you're seeing rifts and layoffs, you're seeing companies being more cautious, you're seeing slower migrations to new software, new hardware, new infrastructure. So you're running a pretty big business at Broadcom. So beyond your GM role though, how are you captaining your ship?

Greg Lotko: So-

Daniel Newman: Should I call you captain?

Greg Lotko: Well, you bring up the captain thing and I know why you're doing it. We should probably clue in your audience, so-

Daniel Newman: Appreciate that.

Greg Lotko: Early in my life I was captain of a hundred ton vessels, passenger ferries that carried 300 or more people off the coast of Long Island. And you definitely learn a lot about navigating rough waters and you learn about things that can happen from within and how to handle them. I've lost all steerage, I've been sinking, I've lost a motor. But you also learn how to handle external events, things that happen to you. I've been out in snowstorms where, GPS is fabulous, it tells you right where you are, but you need radar to figure out where everybody else is and in a snowstorm that doesn't work well. So it is a really great environment to learn on your feet where the stakes are high. You have lives, that you're responsible for. You learn that the most important thing is protecting life.

Just like in business, when a system goes down, the most important thing is restoring it. You can worry about troubleshooting, figuring out what caused it, how to mitigate it the next time as a secondary thing. But you got to get up and running. You got to get the business going. The reality is, in our IT world, it is just like the insurance commercial: mayhem is all around us. We've got hackers that are trying to breach our systems. We've got, whether it comes from a hacker or our own folks, we have rogue pieces of code at times that get injected into our systems. We have subsystems or individual products or processes that might have a defect or break or the automation might not be able to anticipate exactly what the next step is correctly.

So it's a hybrid world out there. We've been talking about that a lot It can be very complex, but using the right tech for the right problem, having the right people in place and the right

processes to surround it, that's what allows you to mitigate mayhem. It's about prevention. And then God forbid it happens, rapid recovery.

Daniel Newman: You bring up a lot of good examples. I like that you talked about cybersecurity, because prevention, mayhem, there's a lot of different types. There's typical IT struggles and challenges. It's not always cybersecurity. But in this kind of current market as things like AI proliferate, with every good technology that comes to help businesses be more productive, there becomes use cases that are nefarious, problematic. And of course you can be sure generative AI and those technologies right now, hackers are trying to figure out how to use it to hack our bank accounts and how to hack our cloud solutions and our software and put ransomware inside. So let's unpack that kind of whole security mayhem scenario. How do you recommend that companies deal with the challenges of trying to stay ahead of this?

Greg Lotko: Well, the first thing you got to realize, and you talked about generative AI, is with every new technology and every wonderful idea that we can dream up for the good of society, for the positives and the goodness that it can bring to our businesses and the industry, there's professional hackers out there that are trying to figure out how to use that same technology to apply it for nefarious reasons. And they're every bit today as unfortunately professional as the good folks that are trying to do the good things.

So it's not about one thing or one strategy to protect data or processes. It is about holistic application of different technologies and different strategies to help secure your environment. So many people think encryption is the “be all, end all.” Hey, if my data's encrypted, it doesn't matter if it gets out, it'll be encrypted. Somebody won't have the keys.

But reality is people are getting ahold of credentials. And if you have the credentials, you see the unencrypted data. So it doesn't matter that it was encrypted. So you need an environment that starts with a paradigm of Zero Trust to only give people access to the things that they need to have access to isolate the access related to a role or related to an individual to encrypt the data on top of that, so that if somebody breaks in and gets somebody else's credentials, they can't get to that data. We've been talking for years about the mainframe being the most secure platform on the planet.

Nothing is foolproof and nothing is secure if you don't deploy the technologies. You have to deploy those measures. And then even when you have all those measures in place, you want to be continually monitoring and tracking the activity, so that when something happens outside of the norm, you can actually track back and figure out where it went awry.

You can figure out who got in, what they got access to and what the exposure is. And then a lot of people on top of that think about air gapping their data or storing copies that have been cleansed. The reality is we all know that's not all the “be all, end all” because these folks that are getting in are lying in, wait. So if you set a strategy that says, I'm going to hold a month's worth of data, they're going to wait til a month and a day. You change it to two months, they're going to wait two months and a day. It's a boon for the storage providers, right? Because you just save more and more data. But you want to deploy each of these technologies and capabilities holistically to provide the most secure environment you can.

Daniel Newman: You bring up a lot of good points. I always think about cyber as sort of offense and defense, and the thing you bring to the attention is I think a lot of companies are playing defense most of the time. And it's because frankly, it's very hard to be on offense. But I do think in this sort of year we talk about the rough waters, the mayhem and the year of austerity that we are facing right now, that every company... It used to be every company's a tech company and it was all about driving customer experience, building apps, scaling your business, growing... And by the way, that'll come back, it will come back. The tech safe line items in our budgets now are things that are deflationary, meaning tech that makes us productive with less headcounts. It just is what it is, and it is something like security. And companies realize it's a board level concern now. It's got to be prioritized at the top.

Greg Lotko: It's protecting your brand, and that's not sexy. Growing your business is–things that consumers can see, but you have to realize the flip side of it. A breach? The data lost? Can damage the brand immeasurably.

Daniel Newman: I mean, Apple made privacy and security kind of sexy, and to their credit, they're probably one of the only companies on the planet that could pull that off. But they did. But I guess what I'm kind of thinking about is, you mentioned something like an inadvertent piece of code. There's offense and defense there. And I guess my kind of thought process and question is how do you prevent that? Is that an offensive thing where it's about making a lot of investments? Is it a defensive thing where you just have better sensing and threat... How do you recommend people actually stop something like that from happening?

Greg Lotko: It is both offense and defense. So, once it happens or there's the issue, you're on defense. You're trying to figure out what went wrong, you're trying to figure out how to mitigate it. But offensively, you should have a change management solution. You should be automating that. You should have processes in your organization, whether they be through tools that are scanning your code or peer reviews that you're doing. You want that to help you navigate around and avoid rogue code. Now the reality is, I have to tell you more than 70-80% of the time when I see an issue at the customer, the first question we always need to ask each other is “What changed?” Because it's usually a change that got implemented that had an issue in it. And that's not saying we shouldn't do change. Change brings us advances and advantages in the company, but when we hit an issue, we need to look at what changed because that is normally the root cause of the issue.

We worked with a very large European bank that introduced a piece of code. We all were working with them through the weekend. They had had a significant outage and we all knew what the one change was. We all eyeballed that one piece of code and said, “Wow, that really looks benign.” When we stepped back a little further and looked at it in the context of everything else that went on, we realized that that piece of code that looked benign caused a call that ended up cascading into many, many, many calls. It did come back to “What was that first change?”

Now you're on defense at that point. How do you get on offense besides automation? Get experts involved early and often. I mean it's something we do. You know I'm in the mainframe space, and while we're the largest ISV in the mainframe space, we haven't created all the software. We work with our customers and say, "Hey, look, any change you have going on in

your mainframe environment–hardware, OS another vendor's software we have experts across the ecosystem. We'll come in and help you review that." And this is something we do as a partner to our customers. This is not a commercial, it's not a fee. Take advantage of the things you have either automated in your environment through peer groups and partners to position you best, so that when you're introducing that change, you are getting all the advantages and protecting yourself against downside.

Daniel Newman: Yeah, a lot of what you are suggesting are probably good practices across all kinds of different scenarios. You mentioned the inadvertent piece of code, but it could be a subsystem breakdown. We've talked a little bit about that. It sounds to me like the playbook ... Of course, there's always going to be some prescriptive differences when you're looking at a hardware issue versus someone getting into your code and there is an interdependence that ultimately takes place. But is there a delta, when it comes to sort of protecting a subsystem-versus an inadvertent piece of code?

Greg Lotko: It actually has a theme that's in common with security, just as I talked about, isolating access to those that need it in their role or by person. You need to think about your system environment the same way, and your subsystems. Isolate the different workloads where they don't have to interact. You can allow the data access, but if you isolate the different components or processes and then you automate failover, you can contain how large that issue is rather than letting it cascade. And then there are technologies that can be deployed to accelerate your root cause determination. But as I said earlier, the thing that I always focus on, our teams always focus on, is the mean time to relief.

Everybody thinks about mean time to resolution. They think about root cause determination, but it's that time to relief that's most important. I mean, think about your elbows bugging you and you go to the doctor and you're there saying, "My elbow's bugging me. Can we fix this?" What you care about first is for it to stop hurting. And if they can't tell you what it is, but they can make it stop hurting right away, that's relief. Now I'm not in pain, now I can relax. All right, let's start talking about what's causing it and how do I avoid it the next time? How do I make sure it doesn't happen? It's that relief that really drives it.

And understanding your overall topology, your overall environment. How systems are isolated, where they interact, the different components that you have there, that's a key component because that helps you investigate everything that's interacting. And then you can use technologies to help you sift through that myriad and blizzard of alerts that you're getting. I mean, I know we're both car guys. If the check engine warning goes on, we immediately pull over, but there's minor alerts in IT that we get desensitized to. We get used to seeing them and we go, "Ah, yeah, that's never an issue." It's like winter comes and the TPMS sensor goes off and it says, “Oh, your air pressure is low. And you're like, "Ah, well, I set it when it was warmer out and there was higher pressure in the tire. That's fine. I can ignore that."

Daniel Newman: There's AI to fix that.

Greg Lotko: Yeah.

Daniel Newman: It's a really irritating one. It's so jarring when the lights are on and you know it's not actually a problem, but it's on, it just keeps reminding. Now I thought when the check engine light, that means to check it by accelerating.

Greg Lotko: Yeah-

Daniel Newman: That's not what it means?

Greg Lotko: That's not the recommendation.

Daniel Newman: Okay. Well that's kind of that desensitization though. It's like, all right, we'll just keep going. And the check engine light's on.

Greg Lotko: You can get faster to problem impact by that, not necessarily resolution.

Daniel Newman: You can figure out just the limits, it's a limit test. So the mainframe sometimes gets somewhat misunderstood of just how important of a role it continues to play in many highly regulated industries, but also beyond that. And when it comes to needing to secure data, keep it private, keep it scalable, resilient. That's the reason people have stayed on the mainframe in many, many industries. Tie that in here, because we talked a lot about security at large, but as companies are moving some of their workloads to the cloud and the public cloud and building hybrid cloud architectures, the mainframe still has a pretty big role to play in both building out business capabilities and also securing.

Greg Lotko: It's a huge role. The platform is misunderstood and misrepresented more often than not. The reality is 70% of the world's transactional data is still today processing through mainframe, and it's only at 8% the cost of IT. I mean, that's a fabulous, fabulous value proposition.

And it's not about “Everything should be done on mainframe.” It's about “Cloud is better with mainframe.” Our overall IT is best when we're using the right technologies for the right workload. And there's studies out there that show it. If you look at the top performers, they're investing more heavily in cloud than the average performers in their industries. And that's not going to surprise anybody, right? You go, “Oh yeah, okay, cloud is the future.” Some people think it's a “cloud everything” or a “cloud only” future. But the top performers are also investing on average 10% more than those average performers in the industry in their mainframes, in their mainframe environment. And it's not either of these in isolation, it's them together– working together. Mainframe to this day is the fastest, most secure platform on the planet. And it's inherent strengths are around security and resiliency to avoid mayhem.

Daniel Newman: Yeah, mayhem like me. No. The thing you mentioned though that is really interesting is the systems we have come to depend on every day and the fact that largely they don't go down. Think about the chaos that would ensue if transactions couldn't be performed or the recent SVB bank run that happened this year. I mean, we know that when our banks go down for maintenance for an hour, we lose our minds. They even have to do that.

And what I'm saying is the fact is that when you put those kinds of critical workloads in an environment that even has 0.0001% higher risk with the volume of attempts and threats, I

mean, it's an exponential difference in the possibility. And that's why a mainframe to hybrid strategy makes so much sense. That's why we need to change the perception because this is still critical. It has a really important role to play, and I don't see that changing anytime soon.

Greg Lotko: The misunderstanding or the misrepresentation is, I'm sure folks on the outside thought, “Well, all we're going to be talking about is the mainframe and that everything has to be the mainframe.” But it's really about how that technology is part of the overall IT landscape. It is not an “or.” It's an “and.”

Daniel Newman: Well, hybrid cloud is an only different public cloud. Hybrid includes mainframe as part of it.

Greg Lotko: Absolutely.

Daniel Newman: I think that's really what we wanted to make sure was articulated. So, let's tie this all together. For everyone out there that's trying to prevent mayhem, give us a few of your best suggestions of how they can approach the situation.

Greg Lotko: Sure. So, design and resiliency from the start, you think about that from code all the way to the customer and everything you do. I am in no way, shape, or form saying that we want to slow innovation. You want to drive innovation while protecting the environment, while protecting what's going on in your IT.

The top performers proactively detect almost 80% of issues before they even happen. And the average performers, they only detect about 40%. So this is a huge payoff and a protection of your brand. Those that are doing it right then have more time to plow it back into innovation. And I think everybody thinks about, “Well, the more I focus on the operational, the less money I have for innovation.” But you reap the rewards. You invest in the operational, you make it secure, you make it reliable. That gets you in a rhythm and then you free up time to drive more innovation.

And everything that we've discussed here today is absolutely a focus for us at Broadcom. Hybrid architectures are complex, but you navigate them with the right technology, the right people, and the right partnerships across the ecosystem.

Daniel Newman: Greg Lotko, I want to thank you so much for joining me here at the Six Five Summit. That was a really important and timely conversation. I think it's one that we're going to continue to have together, but it's also one that I hope everybody out there is really thinking about. Because again, in these tougher periods of time, getting these things right are the major details. And by the way, even when the macro changes and growth starts accelerating, you still to get these things right.

Greg Lotko: And doing it now is what's going to position them for that. I don't want people thinking about this. I want them doing it.

Daniel Newman: Greg, thanks so much.

Greg Lotko: Pleasure.

Daniel Newman: Hey everyone, thanks so much for tuning in here at the Six Five Summit. Really enjoyed having you here. Stay with us for so much more content. We'll see you soon.