Troy Schneider:

I want to briefly introduce our panelists and then we'll give them a chance to say what their name and titles actually mean in sort of the practice of this. Immediately to my right is Amandeep Singh. Amandeep is with Amazon Web Services where he's a solutions architect. Then on the end is Ron Nixon. Ron is with Cohesity where he is the Federal CISO. Gentlemen, thanks for being here. The focus of this is about how to build better data resiliency in the cloud. Obviously, federal agencies have all the usual sort of security and operational concerns plus the larger compliance issues and being perhaps a more attractive target, so it is a complicated path forward in the cloud. We want to sort of get into briefly how agencies can adopt some best practices to approach that. But before we do, can I just ask each of you to give sort of 30 seconds about the role in your organization and how it sort of fits into today's conversation? Ron, we'll start with you.

Ron Nixon:

Cohesity is a data management/data security company. We grew up in the cloud space, but with an emphasis and understanding that you have to be able to do on-prem, as well, so the hybrid cloud environment is probably not going to go away. From our standpoint, we look at your ability to recover and be resilient within that space. In data resiliency, business resiliency, cyber resiliency, however many tags you can put in front of resiliency, but we help you maintain that ability to continue operations despite whether it's an actual disaster or a cyber event.

Troy Schneider:

Good, very good. Amandeep, same question to you. How are you helping government customers with this?

Amandeep Singh,:

The first thing is the way I look at it, resiliency outside of technology, as a person I feel being resilient is a way of life. Imagine that person who keeps getting beat up verbally, physically, mentally and they bounce back. No matter what happens, they bounce back. I think that's the idea of resiliency. No matter what the situation, you bounce back. My go-to mental model, for those of you who like Stallone movies, is Rocky Balboa. There's a line in that that says, "It's not about how hard you can hit, it's about how hard you can get hit and still keep moving forward." I guess that's a lot of what has happened. If you see the rise in cyber events and ransomware, there is definitely an increase in chances that you will get hit, and with so many users, so much data, you really need something which will keep you going forward. What AWS and Cohesity are doing together in this paradigm is they are lifting those gloves up to stop anyone from punching you in the face.

Troy Schneider:

Well, I'm glad you got to that last part, because I was hoping that the focus of today wasn't just prepare to get hit harder in this. But, you touched on just the volume of the data and with the explosion in data that agencies are looking to manage, how can the cloud help defend and provide those gloves up at the head against data pirates and other bad actors?

Amandeep Singh,:

That's a great question. How would I start is applications and data disruptions are inevitable. That reminds me of one of the quotes from Amazon CTO Werner Vogels who says, "Everything fails all the

time." We need to build systems that embrace failure as a natural occurrence. If you look at the current situation, threats have never been more intense. They're only increasing because of the ease of which you can launch these events. Agencies really need to have that capability to bounce back. What AWS does is AWS provides you a number of security features and services that not only help you automate, but also simplify security tasks ranging from key management, storage and sensitive data discovery to inadvertent access. Coming back to the mental model, if you look at this, it feels a little bit better if not getting hit rather than repeatedly getting punched in the face.

Troy Schneider:

Okay. Ron, anything you want to add to that question?

Ron Nixon:

Yeah. Well, I love that Rocky analogy. It's probably going to end up more in a couple of sessions for me. AWS, for a company like Cohesity, and not even just us, so when it comes to data and data management and you've done that scale and scope, so you end up with a lot of noise in that space, so you've got to have the ability to see and touch and deal with your data. Cohesity, from our standpoint, we kind of start in that backup and recovery space and move forward into the environment, up closer to the user as you go. But that data that's in that space, you have to be able to touch it. You have to be able to do something with it.

One of the analogies I like to use when you think about backups is, you've got that safe in your house that you put your passports in and you put your birth certificates in. You lock it and then you close the closet door and you don't think about it again until the next time you come out. Well, the backup environment is a very rich space for bad guys. I used to run red teams for the government and I like the backups a lot. Why? Because I could leave my back door there, but also, it's a good place to have an understanding of what data and information you could actually go after in the production space for an encryption attack for ransomware. It's not being watched to the same degree. Whatever you're looking at for that space, whatever technology you're looking at in that space, ensure that it gives you the ability to manipulate, touch and get insights from that data and information. I think that's really important.

Troy Schneider:

Very good. I'll sort of stay with you for a second, Ron. What about when agencies are working more on, not more on-prem, but where a substantial part of their operations remain on-prem and you're really dealing with this hybrid cloud environment? What are some of the different security concerns then?

Ron Nixon:

I would venture to say that they're not different.

Troy Schneider:

Okay.

Ron Nixon:

Here's why I say that. I've got some physical security concerns. I've got physical environment stuff that I've got to deal with on-prem that I don't have to deal with in the cloud. But when it comes to the way I'm managing that day-to-day and I'm managing that data and that information in that space day-to-day, that doesn't change. And, it shouldn't change because if I'm looking at a different security process for

my on-prem data versus my cloud-based data, then I'm going to have a problem, because when I do have to do some type of security action, whether it's hunt omission or recovery operation, I'm going to have a breakdown in something, so you want to keep it the same.

I want to have the same level of criteria, the same level of compliance if I've got a compliance model I've got to deal with. Those should be the same universally all the way across. I could argue you could go back and you could look at NIST 800-series or if you're talking about the DoD, the DoDI Instructions. They don't change based on how I'm protecting the data versus the cloud. The controls and everything, the main mechanisms are the same. MFA encryption, all of those things, that doesn't change and I don't think it should.

Troy Schneider:

Amandeep, I think people maybe underestimate how much the on-prem component factors into what AWS is doing. Talk a little bit to this challenge.

Amandeep Singh,:

Yeah, absolutely. Just to add to what Ron said, I think the security is an ongoing effort. Having strong identity controls and automating responses to security events, managing multiple layers of infrastructure, and then also at the end, what AWS has done is AWS has made this effort easier by shared responsibility model, where the physical security is AWS responsibility while customer maintains full control of their applications and data. In a way, of course, you have to follow general best practices, keep up to date with those, and then as Ron mentioned about following NIST cybersecurity framework is a start to practicing, bringing those security in practice.

Troy Schneider:

Good. We'll sort of stay with you for a moment just as we talk about external threats. Obviously, there's the internal risk and the Murphy's law considerations to have, as well, but when dealing with external threats, what are some of the security protections that really should be at the top of the list for implementation?

Amandeep Singh,:

When we are talking about external threats, as I mentioned when I'm talking about having those strong identity controls and also apart from that, having a lot of visibility and control of your security controls, how they are being applied. In addition to that, you also need some kind of a logging mechanism, as well. A mixture of all those will help you from the external threat. But at the same time when we talk about resiliency, you also need to think from the point of view of your backups. If your present source is compromised, that something is going to replicate to backup, as well, so protecting your backups and your business continuity operations should be the way to go.

Troy Schneider:

Very good. Ron, any sort of insights there from your red team days?

Ron Nixon:

One is understanding that your environment in the government spaces... The good and the bad about the government is you get the best of it. You get the best bad guys out there paying attention to you on a daily basis, which is not necessarily a good thing. But when you begin to look at that, Amandeep

brought up a lot of the good points about access controls and things like that and you begin to think of some of the common sense mechanisms. I hate going down the buzzword path of zero trust, but concepts and frameworks like zero trust become really important, that ability to make sure that you're authenticating and not trusting anything within the environment.

That crosstalk becomes vitally important, because in the government space you're dealing with advanced persistent threats whose specialty is staying inside of your environment for as long as possible without being found, having those controls at every mechanism within the space, so role-based access controls, for example, even on your data management or even your backups, taking that aspect all the way down into as far as you can so that you have true visibility of what the individuals are doing in the space and what your data's doing in the space.

Troy Schneider:

Okay. I want to go to a slightly less pervasive buzzword, which is immutable backups. You touched on backups being a great place to go live as an intruder. How do organizations sort of build a resilient backup strategy to make sure that when bad things happen, not just the data, but the systems, the business operations are ready to recover?

Ron Nixon:

When people think about resilience, they tend to... I'm a big fan of triads, triangles, so my availability, confidentiality and integrity, I love that triangle. I go back to that because people tend to think about resiliency and they just think about the availability piece. With the immutable data piece, that data that can't be altered, changed, moved, what that gives you is it protects that integrity piece of the data and information. Some of the things you're beginning to see out there with some of the more sophisticated actors, and we see it in the commercial space around ransomware and I know the government's seen it in other places, is a data integrity attack where they just make edits to a database or a file system that you don't really know what they've done to it. They've just made some abstract change, delete the logs for the edit and move on.

Now if you think about something like a realtime tracking system or a fire control system or satellite telemetry, that could be catastrophic. Immutable data sets, that immutable backup, one, it gives you that set of information that can't be changed, but also gives you a reference point to be able to go back and say, "I know this data has been changed. I know it has been altered." I can run that and test that against my production data, for example, to make sure that what I'm running in production is still what it's supposed to be.

Troy Schneider:

Right, good. Amandeep, what are you seeing there?

Amandeep Singh,:

What I would say is it's really important and critical to have those immutable objects and immutable storage, but at the same time, really for the past several years, backup space or backup industry has been focused on just backup, backup window, backup success. What we need to focus is on recovery. You really need to have recovery in practice. How AWS helps is, you can spin up those test environments very easily and quickly. Having those in practice actually depends... We'll actually help you recover. Even if you have the best plan, you might not be able to recover any faster, because when there is an actual outage happening, no one is familiar with it. Having that, and then anyone who's dealing with backups,

there are two things that should be on the lips of every person is RPO, recovery point objective. The other one is recovery time objective. How much data can you lose and how much time the restore takes. I guess at the end, this is really what matters.

Troy Schneider:

I'm glad you went to that, because it's not just having the backups. There is that time to recovery and the visibility in your systems to know what data might have been compromised and what you have to back up, because if the assumption is we must wipe everything down to the metal and start fresh, that's a long recovery time objective.

Amandeep Singh,:

Yeah, absolutely. Partners like Cohesity, they do a great job in that because when you are backing up, they scan for any malware, anything. Then even the storing, they have that inbuilt process that cleans and makes sure that your data is not with any malicious content.

Troy Schneider:

Both of you sort of mentioned in your remarks earlier just the point that failure is inevitable at a certain point. We're managing risk. We're not trying to eliminate it entirely. But, failure's not really very well-tolerated in government and not in Congressional oversight. How do you work with your customers to not only build the resiliency, but communicate that these are our plans and when bad things happen, this is how we're prepared to recover?

Ron Nixon:

That's why recovery is part of that option. There is no such thing as elimination of risk. Any vendor who says, "I'm going to eliminate risk for you," is full of... I've got some expletives for that. There's no way to do it. It is about risk management and it is about mitigating what risk you can, controlling what risk you can. Those are the aspects that you have to make sure that you're bringing to the table. When you're talking to your customers, they have to understand that. Now, a lot of my familiarity is around the Department of Defense. They completely understand that the satellite system or radio system may get wiped off the map. That's an expectation possibility, but then also taking into account those other pieces about, "Well, you know what? The same thing could happen to your data." I was glad you brought up that blast radius piece, because sometimes you're not in a position where you can just wipe the slate completely clean and you need to be able to understand what you can actually recover and what you need to recover.

Troy Schneider:

Very good. Well, we are almost at time, but Amandeep, I want to give you the last word on this.

Amandeep Singh,:

Yeah, absolutely. At AWS we know building strong foundation is the key to resilient cloud architectures. AWS provides over 200 fully-featured services across 99 availability zones and 31 regions across globally. If you look at these regions, these are build of multiple availability zones, which are further divided into two or more data centers, each of which owns its own facility with redundant power network and connectivity. Having that balanced infrastructure is already out there for you to use, so levering that infrastructure gives your systems out-of-the-box resiliency.

Troy Schneider:
Very good. Well, gentlemen, thank you for sharing your time and insight today, really appreciate it.

Ron Nixon:
Thank you very much.

Troy Schneider:
Right.

Amandeep Singh,:
Absolutely. Thank you so much.

Troy Schneider:
We'll go-