ANNA: This week, Stan and Chris revisit a conversation they had with Jamil Farshchi, the Chief Information Security Officer at Equifax. Jamil has had a distinguished career in information security transformation: he was the first ever Chief Information Security Officer at Time Warner, and worked with both Home Depot and Equifax to build safer networks after their respective cyber breaches.

We wanted to revisit his conversation after the recent cyberattack that shut down the Colonial Pipeline earlier this month.

Jamil is a thoughtful leader who shares the importance of building culture in our teams, and discusses why security is *everyone's* responsibility in an organization - a conversation that's as relevant now as ever. Thanks to Jamil and his team for taking the time - now, over to the discussion.

CHRIS: So I'll just, I'll dive in and Jamil, I just want to thank you for taking the time to join Stan and I here for discussion. To get us started, an you just walk through a bit about your career? How it started, how you got into this, this area and where you are now? And we'll sort of go from there.

JAMIL: Sure. It's sort of interesting journey, I think. From a kid I've, I've always loved technology and you know, I ended up winning my middle school science fair because while the other kids were, you know, building volcanoes and doing experiments… I coded up a Frogger game clung and ended up… I was just a computer geek from the start.

And then when I got into college, I started getting into the security aspects of it more. And I was playing around one day and ended up compromising my school network, actually. And so, I could have used this for nefarious purposes, but instead I was really excited about what I had accomplished and I'm like, “Holy smokes, there's a meaningful vulnerability here.”

And so, I took it to the Dean of my college and out of it, I ended up getting a fellowship to do it for the entire university. And so that was sort of my first foray into the security industry. And then from there, I went off to NASA for my first job out of school. Had a great opportunity to work with some of the most innovative technologies and brightest minds I think around. It really served as a great foundation, I think for me throughout the rest of my career. And then moving forward, I've been head of security for Los Alamos National Laboratories, protecting many of our nation's most secrets data ets as it relates to nuclear weapons, $7 trillion worth of transactions a year when I was at Visa, media and entertainment when I was at a Time Warner.

And then I was brought to Atlanta where I'm at today by Home Depot, after their big breach, they had to help turn around that program. And then the breach occurred at Equifax. And so, they brought me along to help drive the transformation and rebuilding of the company and this program as a result of it.

So, I've always been in security, always been in risk management. I guess I sort of gravitate towards crises and opportunities to be able to make big change. And it's, to me ,it's fun. I'm passionate about it and it's been a nice ride.

STAN: That is fascinating. Let me thank you for being on today.

I want to start with leadership and then we're going to get a little more broad. But when you describe your history and I was most familiar with the Equifax experience you're brought in and there is a crisis there's sort of wreckage, there's a little bit of shock across the organization. Talk about coming in, not from the technical standpoint, but from the leadership standpoint, how do you have to come in? How do you think about that?

JAMIL: Yeah, it's a challenge. And I think I think a lot of times folks sort of dismiss that aspect. I'd like to look at: what's the root cause? What's the … how are you going to put out the fire and things like that, but they forget about the human impact.

And, you know, when you come into a situation like this, oftentimes, you're walking into a team that's demoralized. They've been working 24/7 for the past several months, scrambling to try to get as much done as they possibly can. And they're scared, right? Because there's a lot of uncertainty out there where they're, "Hey, are we going to be able to do what we've committed to?" "Am I going to have my job tomorrow?" "I've got this new person here that's, that's going to lead the program."

And so, I think one of the most important facets of coming in is really emphasizing the culture itself. And I think look, I'll go back… I field these kinds of questions all the time as it relates to hey, did you… how has your patching program? How has your certificate management? Did you have assets and asset inventory in place?

And people use those as a mechanism to try to figure out what the root cause is, but going all the way back to my very first job at NASA, it was 2003 and it was the most devastating organizational crisis I've ever experienced. It was the Shuttle Columbia disaster. And, and in that, as I'm sure you're well aware, upon re-entry the shuttle - because the wing had been damaged - he was able to penetrate the wing and then it ultimately disintegrated the entire shuttle and we'd lost seven amazing people throughout that event.

And then the Columbia Accident investigation board came in after the fact and when they did the review, sure, they came up with all these technical issues and things like that that were problematic, but the most compelling thing, and the thing that's stuck with me ever since 2003, when this occurred was the fact that they said that an accident at NASA was inevitable.

Irrespective of all these other things, it was inevitable because of the culture of the organization. There wasn't the right level of transparency, there wasn't the right low accountability is established. And so, I've taken that with me across every organization that I've been. And it served me extraordinarily well, as it relates to stepping in after a crisis, because it's not your patching program, it's not this issue or that issue. Those are all manifestations of the broader

problem typically, which is the culture of the firm. And I think that if you get the culture, right, you can even have a mediocre talent level on your team, but you're going to be positioned to succeed.

Whereas you might have the best, most talented, skilled individuals on the planet… if your culture's broken, you're going to run into some problems and you will not be able to ultimately achieve what you're striving to do. And so that's really the number one goal whenever I step into any organization, the talent processes, technology, strategy, those are all important, but hands down, the number one focus for me is culture.

STAN: If I could follow up on that, because I find this so critical. I was in the National Military Command Center in the Pentagon when the Challenger accident occurred. I was the vice Director for Operations. I'm not a space guy, but we were obviously tracking that very closely – and when it occurred, you think about that and you start to say, "Okay, what's it going to take in an organization to do the kind of reflection, self-examination, to really determine what the, what the challenges are? Maybe what the issues with the culture are. How do you address that with an organization when they've just, as you mentioned, they're a bit frightened. They're a bit in shock.

JAMIL: I think you lead by example for starters, right? I mean, at the end of the day, you can't just take one singular approach to changing the culture and you can't expect that the culture is going to change overnight. And so, one of the things that we did here is we established a series of measures, spanning incentives, spanning organizational structure, spanning communication.

So, we changed the reporting line so that my role reports directly to the CEO, one of the first firms of our size to do something like that. We established incentives so that all bonus eligible employees have a specific security component tied in. And if we don't meet our targets, then everyone gets a meaningful…that's pretty, pretty strong incentive for anyone, anyone working. We built in controls around capital allocation. So that security and risk reviews were done. So, you have the right level of oversight for all of these things.

And then we did put a full court press on communication throughout the organization to make sure that everyone understood that security isn't just security's responsibility. It's responsibility of every single person within that organization and all the actions and decisions they make on a day-to-day basis. And so, taking that multi-faceted whole of company approach I think allowed us to be able to, to win the confidence of the team, establish the right longer term direction, and then ultimately allow us to get to where we are today, which is a leader in the security space.

CHRIS: Can I build on that a little bit, maybe blending those together? You've been at, in this space for almost 20 years now. How are you, or are you seeing the view around your space inside of a large organization change on the other executive level? And if you hit walls where people don't understand that it really comes down to the human dynamic, how do you start that conversation and make people aware of how critical that is?

And it's sort of near and dear to Stan and my background in that the special operations community, which is often seen as this sort of… it's a bunch of sort of cyborgs. They go out and

do missions… no, it's real people with real families behind them, the same stresses that everybody else has. And if they're not optimized as individuals, then you can't the missions there. Aren't going to be successful. I'm just curious how you approach those discussions.

JAMIL: Sure, first off, I would never suggest that what I do has is anywhere near as stressful as the work that you, you two have done in the past. Not even close. But, but nevertheless, there are many stresses involved with it. And I think communication is one of the most important fastest, especially because by almost by definition, security tends to be a fairly technical area. And unless you have some background in it, it's difficult for other folks to understand it.

I also think that we have a challenge where… because our, our natural role is more of a defensive one, people sort of associate with (I'm a big football fan) they associate it more with like linebackers. I would argue that we're less like linebackers in the football analogy and more like offensive lineman.

Right? We protect the quarterback. We protect the running back. We protect the team to be able to advance the ball, but we also open up holes and opportunities to be able to drive the business forward. And so, I try to use that lens and that framing, whatever I talk to the executive teams and communication is so important to not make it a technical thing. It's a discussion about risk. What are the potential threats? What are the vulnerabilities? What are the implications of those vulnerabilities, versus is it a cross site scripting issue or we didn't patch this particular asset?

I think if you go down that path, we fall into the trap that I think a lot of security organizations do where you're just that cyber guy, you're just the technical folks on the side, in the corner, instead of actually being a true business leader and helping to enable the organizations. If you walk like a duck, and talk like a duck, and you're a duck. But if we walk like the business, and talk like the business, and really try to drive enablement, then it puts us in the best possible position to succeed.

STAN: So, I'm cheating now because I'm writing a book on risk and you just use the "R" word. So, I want to grab at it. One of the things we found is it's very interesting because in some organizations where they create a chief risk officer, like investment firms or a security officer for information technology, there's something called "moral licensing," which everybody else says, "Okay, I don't have to worry about cybersecurity, because that person's responsible and if something goes wrong, that's their problem."

How do you communicate the problem with that to people?

JAMIL: You're spot on. I mean, it is fundamentally… which is why earlier I was saying security is everybody's responsibility. I mean, I should have said "risk is everyone's responsibility" because it fundamentally is.

But it's one of the biggest hurdles that we have to overcome. And I think it starts from the top. If the board of directors, if the CEO, executive leadership team don't subscribe to that same notion,

but it's never going to happen because it is then just the security team's job. It's just Jamil and his team, and that's all that's going to be.

But once you build that into the fabric of the organization, into the DNA, like focusing on trust, focusing on risk, building in the appropriate oversight rigor, then you're able to be able to define accountabilities for who's driving it. So when there is an application that goes into production that has vulnerabilities in it, it's not Jamil's team's fault, right? Necessarily. It's probably on the technology side. If the business goes through and fails to comply with certain regulatory obligations, then it's going to be their responsibility to do it. But unless you have that concept built into the fabric of the organization, the appropriate processes to be able to support it, it just falls apart and then it just becomes security's job and we're going to do whatever we want.

I try to focus heavily on metrics to be able to demonstrate data. So, it's not just Jamil as you know, the "Boy Who Cried Wolf." But we can leverage data and then we use it in an attributable way. So, we can marry that up with the individuals that are driving that particular risk. A simple, simple example would be your security awareness training, right? We send them test emails out to the entire workforce on a consistent basis that tries to basically trick them. They look just like an adversary's phishing email they would send. Users either click them or they don't click on them. We aggregate all the results of this. If you reported it, if you opened it… all of that data is there, and then we can divvy it up and then show it to the business unit leaders, to the individual owners, and it helps to be able to drive that culture.

And the beauty of it is you also get the sort of competitive aspect where, you know, we sent one out the other day and my CEO's like, "Oh, you know, I could have done a little bit better on this. What I gotta do… I gotta, you know, up my game for next time." And then our head of one of our business units saying the same thing.

And so it really helps and it doesn't happen overnight, but if you drive those processes and you drive that level of engagement and you have the support from the top, that's the only way I've seen to do it. Otherwise, it'll fall apart and it ends up being a team of one.

CHRIS: Jamil, how much differently are you grooming up and mentoring young leaders in your space than you were 20 years ago? Is that changing as well?

JAMIL: Yeah, we have a huge problem with supply and demand in the security space. You know, you can, there's a variety of studies on this, but it ranges anywhere from 3 million to 3 to 5 million potential roles that are out there that we just don't have the supply for right now.

And so, I think it's incumbent upon everyone in this space to try to work, to develop and mentor folks, to be able to prepare them for what ultimately we're going to need. But that said, I think that one of the biggest challenges I think we have in the security space is similar to what the general was referencing earlier and that we, we don't do a great job of being able to talk the talk as it relates to the business. And so we ended up being siloed out as a result of it.

And so, when I mentor folks, one of the things I try to do most is first exhibit the behaviors that I think are critical to success: driving strong communications, holding people accountable, having the right sense of urgency to drive things to fruition. But I also try and every mechanism I have, whether it's through my presentations or it's through the metrics that we use or whatever, to be able to help slowly build people up, to understand what is ultimately needed for the next level, to be able to build them up. We also have a variety of other programs – I'm a huge fan of apprentice programs to be able to learn the core fundamentals of different security areas, rotating people around at a different capacity so you're not just an expert in one specific domain, like data protection, for example. But instead you're able to go across the gamut and do threat intelligence and sort of intelligence understand the cyber aspects, risk management, and so forth.

So, it's a, it's a huge focus for me personally. And therefore, a major area for us as a program as well.

STAN: How much of your focus is outside the firm that you're in at the time, you know, clearly we think of security as locking the doors and the windows guarding the walls sort of thing. But I think of cybersecurity is more broad. How much of your time is going out to other organizations linking with them, that sort of thing?

JAMIL: General, that's a great question. And two parts of this one. The first one is it depends on the organization. Every business that I've been with is different. The strategies we employed at Los Alamos are completely different than the ones that we have in place here at Equifax. And so that's a part of it and your business model. So, Home Depot more of a B2C firm here, we're much more of a B2B. And so we take a different approach to it.

But I think as it relates to outreach it's essential at all levels, no matter what your strategy is, at least as it ties to getting intelligence and getting best practices from other partners out there, we've made a concerted effort to partner strongly with the FBI, for example. In fact, I was just talking to them last week for the FBI Academy. Are different customers out there getting in with the different groups, like FSI SAC and things like that?

Building up coalitions amongst likeminded individuals and organizations, to be able to share information and best practices. DHS, we go, just go down the list. And the reason we emphasize this so much is because we can't fight this fight alone, right? If the, if the military arm of, of China VLA is, is attacking us, you know, our team by itself… we're not going to be successful. We're only going to do it collectively as a group. And we've built up really strong coalitions amongst different firms. And we get threat intelligence and insights from them. We share it back out, but I don't think you can be successful in this world, in this day and age, in this space, unless you partner aggressively with different firms.

CHRIS: You mentioned China there and some, some major, you know, state-on-state actors and threats. What do you see as the major areas in the next three to five years that really give you pause? Areas that, where you're concerned that maybe we're not collectively keeping pace with what the, you know, the threats that might be around the next corner?

JAMIL: It's a tough space. I mean, if you look at the, if you look at it, what's happened in our industry over, if you look at business in general, over the course of the past, even 10 years the digitization of assets and the reliance on technology is certainly far greater than it ever has been. And I would argue that there's virtually no firm out there that can, that can competitively exist without leveraging a meaningful technology stack and digital assets. As a result of that though, we have a tremendous amount of additional risk because it's a very attractive target and you don't have to be on our shores to be able to get it - which is why we see these attacks on Main Street here from these other nations states out there. So, I think that the threat is real. We only see it continue to escalate. If you look at COVID, just over the past couple of months, the rate of attacks and the threats out there have, have increased demonstrably.

Yeah, we're still fighting the fight, you know, on our turf here, but it's, they're knocking at our door. What concerns me the most is the national strategy as it relates to cyber defense and particularly not just the defense aspect, but also the continuity, the economy thereafter. There's… I'm not going to say that there will be one, but there's, it's plausible that there will be a cyber pandemic, right? I mean the level of integration and reliance on the technology we have through our critical infrastructure is immense. And it's a very attractive target.

And so, the biggest concern for me is our ability as a country, not just the government, not just the private sector, for us to collectively come together and establish what that strategy is going to be and put the pieces and parts in place through law to enable us to be successful. And I think I was encouraged - I think it was March or April of this year, Senator King and Representative Gallagher co-chaired a Cybersecurity Solarium Commission Report. And it actually outlines a very materially strong strategy with actions as well to be able to help us position ourselves for success in the event that something like this were to occur.

And so, I think that there some progress there and I'm encouraged by it. But, we still have a long ways to go before I would feel that we're in a position to be able to effectively not just defend, but also persevere through an attack like that.

STAN: Well, your task now is to make me feel better. So, I've been on a couple of commissions here recently studying the COVID-19 pandemic and looking at how we can be better prepared as a nation for a similar kind of event, not exactly. And thing that, that has come away for me in COVID-19 is that we actually understood the potential problem very well. The exercise Crimson Contagion actually laid it out pretty clearly. We understood and had a plan on how you respond to this kind of a challenge, but we didn't resource that plan. And then in the moment we didn't execute it. And that was very disappointing. You gave me a hint that disturbed me a second ago, but if I drew that conclusion on cyber. Where would I be wrong?

And again, feel free to lie and make me feel more comfortable.

JAMIL: I wish I could. First off, I can't lie to you and it would be, it would be such a tall tale if I were to lie… I don't know if it's even remotely believable. I feel like there are a lot of organizations and there are a lot of individuals out there that are trying to do the right thing. There's no question about it. I think there are good, good things in place. We've improved

demonstrably as it relates to our information sharing. We've made meaningful investments in critical infrastructure. I just don't feel if you're on the front lines, like we are day-to-day, it just doesn't feel as if we have…. we're prepared to the degree that we need to be.

And I think COVID is a great example of, you know, all the things that can go wrong for something that you had already predicted and planned for. And so, I think it really boils down to being able to be adaptable and being able to effectively execute on the plans that have been defined. I mean, I think when you look at what we've done at Equifax, one of the things that we heavily focused on was our crisis preparedness. We do crisis exercises with our board of directors, with our executive leadership team all the way down through the entire ranks. And we do this, not because it's fun or because we, you know, we have a bunch of free time to spend doing it. We do it because we want to be prepared to ensure that if something were to happen, and anything can happen, that we're in a position to be able to respond to it.

And we can't predict what those things are going to be. And so, we've developed a dynamic way to be able to solve for some of these challenges where we don't have a book of, you know, 200 pages that you have to thumb through to figure out what your role or responsibility is. We test them over and over again with different scenarios to be able to build in that muscle memory so that we can be adaptable. We can be dynamic irrespective of we didn't plan on COVID happening, but you know what, when it did occur, we're able to assemble the teams, make meaningful decisions, drive out strong communications, and we didn't miss a beat. Our technology was in place ready to it, ready to go. And so, I think if anything, we serve as a good example of what can happen when you were prepared and you're able to be able to, to continue and operate your business.

I know we're a microcosm of what you were referencing there, the broader economy, but I think it's definitely possible. We just need to apply the resources to it and make it happen.

STAN: Can you take in the room on one of those? I'm sorry. Can you give us a sense on what one of those exercises feels like in the moment?

JAMIL: Yes - and it depends on the exercise. So, we come up with all kinds of all kinds of various scenarios and they're always scenario-based. We don't just make them generic. What we try to do is we highlight… we start pretty simplistic, like standard thing that would occur, right?

“Hey, we have an outage on something” or whatever. Or, “Hey, there's a, someone's claiming that that Equifax has been compromised” or something like that. And then we just build upon it. And what we try to do is focus on all of the different organizations and individuals, they would have to be to play a part in it, whether it's communications or it's legal or it's finance or sales teams or it's operations, it's a board of directors, whomever.

And we, we gained these things out and, and they're the, I think the best part about them is how much you learn as you just go through the decisioning process. Who's got point for this particular decision or how are you going to navigate these two completely competing goals that you may

have in terms of making sure that you're communicating in the right timeframes versus being able to make sure you're keeping your systems up or your services and products available?

So, they're there. They're out. I think that they've generated a tremendous amount of, of lessons learned. We document those and we continue to build upon them. But they can be pretty heated at times, as soon as you go through that learning process. But it's all for the better. It helps us work better as a team and it helps again, prepare us for whatever may come in the future.

CHRIS: Can we pivot just a little bit to the, with the current crisis? When, when it became clear, you know, three months ago that we were going to go into this very distributed workforce for at least the foreseeable future, someone in your position, what was running through your head? Like how much more risk did you see that putting into the equation than when everyone's centralized? And are there lessons there that you think we need to learn if we can imagine like the next wave of this beyond the immediate? Is this going to change the way that organizations see this potential and are they gonna have certain factors built in down the road?

JAMIL: I, my expectation is that organizations across the board will be far more prepared for crises in general, as a result of this, it'd be hard for me to imagine a scenario where that wasn't the case, because we've all now been through once. Just like when you go through a breach that if you have another one, then you sort of know what to expect and you can, you can gain it out.

That said, you know, when this, when this one hit, I was, I was surprised. I didn't expect. There to be a, you know, a pandemic. No, we had gone through and done tests on a variety of things. We got, we got lucky even in one of our tests last year in November, we had tested the cyber team itself, not being able to come into our fusion center that we investigated.

We spent $10 million in this facility to be able to drive communications and collaboration and all of a sudden, well, what if we can't do that anymore? So, we'd actually tested some of these components out. But I think the other part of it is that we, we knew upfront as we were going through our transformation effort here at post-breach we're spending, you know, a billion and a quarter dollars, to the communication was going to be absolutely critical, that the future wasn't going to necessarily be like in, in the office all the time. That's just the way the workforce and business has been evolving over time. And so, we had put in a lot of the right investments, technologically, to be able to solve for it.

But I think that as we move forward, there's going to be a balance. There was a tremendous amount of positive uplift when people first started to work from home.

I was looking at the data and I mean, week after week, I'm like, “holy smokes. Our productivity is off the charts here. This is insane.” And so, it leads you initially to think, well, man, maybe we don't need offices at all. I mean, I'm sure my CFO would be really excited about that because he has to pay for the, you know, any of the capital fees on that way or the lease and stuff like that.

But, but the reality is that over time people need to be with other people. And so we took an approach where it's more dynamic. And so, we said, look, “Our officers are going to remain

open. If you want to come in, if you feel safe to come in, we're going to put it all the possible protocols around it. But you have the flexibility, the ability to be able to come in, if you so choose."

And what that's done is giving the workforce the option, helps them because if they want to come in, they can, we can work in collaborative together in the office as normal. If you don't feel safe, if you don't feel like it's the best decision for you, then you can operate from home. And I feel like organizations will migrate down more of that path and be more open to remote work. And quite frankly, even potentially take advantage of some of the opportunities there were. Maybe where you will only be able to find talent and focus on Atlanta because that's where we are. Now, you can open it, open the aperture and leverage talent from all across the globe potentially, and get the best of the best wherever it may be irrespective of where your headquarters is located.

STAN: Jamil, you hire young tech talent for tech training and protect talent, but a percentage of them need to be leaders. And at some point in your career, I'm sure when you first started, you thought of yourself as a technician, and then at a certain point you realized when I go to work, I really spend all my time leading. Talk about your transition and then about what it's like ffor the people that you lead, how do you make that work? I

JAMIL: It's a great question. My, my critical moment was, it was actually back at NASA. When I came on board there, I was that technical guy, and I was an individual contributor and I loved it and I love tinkering with other stuff and I was a pure play geek.

And then I got the assignment to lead the certification and accreditation for the entire agency. FISMA - it was at the first year of FISMA. And I did that reluctantly. I was like, "ah, this is compliance. I don't really feel like doing this," but I did it anyway. And I had a team of, I think it was around 40 people.

And throughout that process, it took about a little over a year, I think it was. And throughout that process, I got so much joy, not from what I did, but from the accomplishments of all of the people on my team. Seeing them, seeing it come from this group that was just pulled together from all the different NASA centers, didn't really know each other pulling, pulling them together, focusing them on this core objective, and then seeing us accomplish it.

And, you know, I didn't do anything meaningfully technical in that capacity. I just led and I got so much satisfaction out of it. That I realized at the time I was like, look, this is, I don't want to go back to just being the "hands on keyboard" guy. I wanted to be able to do, and we did a good job. So, I'm like, I think I can do this. So that was a seminal moment for me. And I've tried to position people as I see them throughout my daily working life for people to, to have that experience. Some people it's not for them. They, they just, not that it's bad thing. If you don't want to be a leader, you can do an outstanding job as an individual contributor and create a tremendous amount of value. But you have to afford people the opportunity to be able to be in those positions. And it doesn't have to be high stakes, critical risk kind of roles.

But give them the opportunity. And in my experience, the ones who really dive into it and like it tend to really succeed. And then you serve, you organically build that next generation of leaders and then you keep stacking on and just give them more and more. And until they get to the point where you're like, all right, that you're ready to go and you're going to always learn. Never feel like you've like you've mastered anything because things change constantly. And if, as long as you're humble and you're going to continue to adapt and develop, then you're in a great position. And that's what we try to emphasize here.

CHRIS: Jamil, when you put younger folks into those positions, do you do you explain to them, "Here's the leadership opportunity that you can learn from?" Or do you let them self-discover?

JAMIL: I mostly tell them up front. I say, "Look, this is a great opportunity for you. And I talk about the value proposition and the excitement of whatever it may be. And I, for these projects, these are typically things that I am enamored with myself. And so, I do that on purpose because I know that that will, that will drive me to be more engaged with them and help carry them and help them help guide them along the way.

So, I do afford them that, but I don't go into it too much because if you do, if you provide too many guard rails and too much handholding, then they're not actually, they're not actually learning what you need to be a leader because they're just following your own instructions. And I don't think that the role of a leader is to just go through and explicitly define what the other people need to do.

I'm not going to be picking technologies. I'm not going to say this is the right specific strategy for access control or whatever it may be. I want to hire these people to do their role. And that's what the role is. And so, I want them to be able to step into it and certainly I'm going to guide them and provide my two cents when necessary. But ultimately, I think the key measure for a successful team is that I can go away and this team is going to continue to operate at the exact same level that it has been because they understand what the critical factors are for success. They understand how to analyze and diagnose a particular problem and establish a meaningful strategy and then drive the resources necessary to right, execute on whatever that plan is.

STAN: Let me, gets something very personal - if you don't mind. When I first met Chris, he was leading SEALs on combat operations. If he got it wrong, people that he cared about died. Although a CISO, people don't always think of it that way, if you and your team get it wrong, the consequences for an organization can be pretty huge and you know, want to get on the front page of a paper, you know, be the CISO when something bad happens. How do you deal with that? Because that's stress, I mean, that is every day kind of attacking stress.

JAMIL: Yeah. It is stressful. If you look at the data, people in my role have an average tenure of 18 to 24 months nowadays. It's abysmally low. And I think it speaks to the stress of the role and it's challenging for sure.

What I do, is I try to focus on my own discipline. Like this is what keeps me saying quite frankly. And, you know, I get up, it's funny. I was, I've read stories about you, General, and I

admire it because I'm like, well, I'm not quite to the same degree. I've… I do some of the same things.

I get up early every morning, try to do at least by 5:30. I start my workout regimen. This is when my team laughs at me because they get random emails and texts from ungodly early hours in the morning. I tell them they don't have to respond right away. Wait until later on. I try to eat healthy and then I try to focus on enjoying the ride.

We're look… the stakes are high. Bad things can and will happen. But if we're wearing that stress on our sleeve, we're not being good leaders because our teams all see that. Every single day. If I come in there, they're going to live that stress and they're not going to perform to their highest performance levels. And so, I try to balance myself and keep myself healthy, exhibit a meaningful level of discipline to be able to show the rest of the team that, “Hey, this is how we can get it done.” And then I try to guide them to the best degree possible by maintaining my own composure and ensuring that they know that they have a leader that is right there with them day in and day out. And that we can get anything done irrespective of how much of a hurdle it may be.

CHRIS: I think that's really well put, Jamil. One final quick question. What gives you optimism and all this? I mean. it's a pivotal time for all of us on industry and beyond on a longer time horizon. What good do you think is going to come out of this?

JAMIL: I think that's, I think we've all learned a lot. I think that's the key takeaway and my hope and my expectation is that given all that we've learned, given all that we've experienced, we've not only learned what we can do better, but we've also learned definitively that we can persevere through just about anything. Right?

I mean, this is a global pandemic people didn't expect it for the most part. And we've been able to persevere through it. Yes. Has there been bad times, there have been decisions that, you know, the things that we could have done better? For sure. There's no question about that, but I think collectively as a country, shoot as the world, as a whole, we can learn from this and put the right resources, put the right thoughtfulness behind it and do better and just continue to improve.

We can't expect perfection. We just can't. But as long as we can learn from the things that we didn't do, as well as we could have, then I think it sets us up for a lot of success in the future. And that's, that's my hope. And that's my expectation for, for us all.

STAN: Wow. Well, let me start by just thanking you for your time today. I was that kid making volcanoes. There lies the problem. Right. But, thanks for your leadership. Thanks for what you're doing, because it makes a difference. I mean, the nation is really just the amalgamation of all people doing good work, keeping us safe in so very many ways. And so, thanks to you and your entire team for what you're doing and for your generous time today.

JAMIL: General, thank you so much for everything you've done and you continue to do it's been my honor to be here today. Thanks.

STAN: Thanks. Have a great day.

CHRIS: All right. We wanted to rerelease this discussion with Jamil for a few reasons. We've got another conversation with him coming up this week with a small gathering of friends. So we were sort of revisiting our discussion with him from a few months ago, but even more importantly, the recent colonial pipeline, cyber ransom attack here in the US that anyone listening to this would be familiar with the implications of that, which is really just the tip of the iceberg of what's potential in this space.

So Stan and I just wanted to get Jamil's thinking back out there because I am in a space that I am a novice inside of. He is one of the deepest thinkers and most impressive resumes you'll ever find. Stan, one of the my takeaways from re-listening to our conversation, with Jamil, is there is… we have to make this shift as a society and industry as a government, but it is really a fundamental seed change in how we think about a new type of problem. One that there are people like Jamil that are deeply immersed in and others where most of us know just enough to be dangerous. So curious, especially with the recent ransomware attack, any reflections on sort of driving through that level of change?

STAN: Sure. I think earlier in our lives, you know, there might be a hack and your laptop would be screwed up for a while. He couldn't play computer games. And then a week ago, when the Colonial Pipeline got hacked, you couldn't get gasoline in many parts of the east coast.

So suddenly our physical mobility has been constricted by a cyberattack on a pipeline. And then we find out recently that in fact, the CEO paid $4.4 million in ransom to DarkSide, the hacking organization, so that he could free it up. And it, it brings me back to history. In 1797, French, our earlier allies in our Revolutionary War had started harassing American shipping and the rallying cry in the United States became "millions for defense, not one cent for tribute."

And then as American commerce started being hit by the Barbary Pirates, in fact, the modern United States Navy was launched with the construction of six frigates. And that was because we understood that the United States is a trading maritime nation. Our network had to work. And in those days, our network was our ships go in places and taking trade.

Our network was essential to our society functioning. I think that's where we are now. I think what you meal points out is at the very basic level, our society functions because it's connected and when those connections are threatened, we have an existential threat.

CHRIS: Yeah. It's a great analogy. Fun fact for the listeners: my wife is from St. Simon's Island, Georgia, which is where the live oak for the six frigates came from for those that are, the history wonks out there. One of the things that comes through whenever we talk with Jamil is his, I mean, he's a brilliant technology leader, right.

But he doesn't talk in 1's and 0's. He talks about the human factor in all of this. Right. And you know, my, again, "I know enough to be dangerous" sort of knowledge of the hacking world is

there's not some mysterious black box that just, you know, creeps through the connected wires and figures, this stuff out. These are human connections that allow hackers to enter a system. Um, and that, and that's true in all of these cases as, uh, as they unfold and his. His point is always, we have leaders in this space, in the cyber realm and inside of any organization, need to have a role in the leadership of the organization to understand, to create a culture of understanding around that. There's not some tech person that's going to show up and fix the problem - that's too late. They're already inside the wire when that happens. So, elevating this conversation to the human realm, is critical.

I think we're starting to get it, but I think leaders like Jamil would say we're still very shy where, where we want to be. Just curious if that got your wheels turning as well when you listening to him talk.

STAN: I really did. And not just inside the organization where you need people to follow certain practices and understand it. But when you extrapolate further, I could argue that the decision by the Colonial Pipeline CEO should have been a national decision.

Maybe it should have been a US government decision because in reality, the effect on our economy is far greater than one pipeline company. And so, when you talk about people, it's leaders having to understand. People with an appreciation of the interdependencies of these things, because that's how the decisions have to be made.

As you say, they're not technical fixes. There's a technical capability we have to have, but there's a very human understanding and a strategic resolve that's necessary. Yeah. The imperfect analogy that always runs through my head is, you know, as a parent taking your parents to a pool, right?

You still teach your children how to swim, just because there's lifeguards, you know, just because you have an IT department that can come in and help figure these things out, it doesn't mean it doesn't absolve us as leaders of making sure that that frontline awareness is still part of our culture.

One last thing that I'd love to bounce off you. I don't know if the comparison resonates with you, but, when I was on your staff, when you were running the counterterrorism units around the world, anytime we would, I was with you and you would visit an outstation or wherever it was. You'd spend time, obviously with the operators and leadership and, and on the mission side, but you'd always make an important point to spend time with what we would call in the military the "six department." There's one, two, whatever codes in the military, and six is always your communications department. And so, the there'd be these young folks in the back of the headquarters, wherever with, you know, antennas and wires and stuff around every direction.

But you made a point to check in with them and explain if I recall correctly, your view that that was the nerve center that connected us around the world. And you didn't check in and say, "I appreciate you bringing all the laptops," or whatever it is. It was a discussion about them as a human network. "I appreciate you all. Stay maintaining these relations, the ships around the

world with all these other communication hubs, because if it wasn't for you, as people in the middle of this, we would be completely disconnected from one another."

So it's much more than just the transactional skill of being able to plug in and make this high-speed connection work. It's your ability aas humans to understand the importance of that and stay connected. And I could tell that they were never spoken to like that. And it, to me, it jumps out as an analogy here. And the point that I think Jamil tries to make is leaders need to understand who's in that tech department and give them a voice inside the broader organization.

STAN: Yeah, it's so true. I smiled when you started that because I learned over time that the difference between getting the communications you need is always the person. Remember, we were an Addis Ababa by Ethiopia, and we had to stay in this hotel. We were doing important meetings and the communication couldn't get the right satellite shot from the room that they'd been put in.

And so, I walked in the room to see whether they got communications up yet and they had duct taped a chair from inside the room out, so they went around the corner of the building and it could aim at the satellite better. We were about eight or 10 stories up. And the plan was for one of those communicators to sit on this chair held by duct tape to this rickety balcony, so that we'd have communications.

And I remember stopping the plan, but it was exactly the kind of communicators you need because at the end of the day, it's wires or other kinds of technology, but that's not a network. Those are only enablers that allow people to connect. And it's people who make that stuff work. And so, the cultural part of that is the difference.

CHRIS: I remember that night well. And I can guarantee you, you came in that room just in time.

STAN: That's right.

CHRIS: Seemed like a good plan. Well, we really appreciate Jamil and his leadership in this space, which is obviously growing increasingly important to all of us as we felt over the last few weeks. So, thanks to him, thanks to his team. And thanks to all of you for listening to this discussion.