Cisco Cloud Unfiltered Podcast Series, Episode 9: Branson Matheson

Branson's currently a Cisco cloud operations engineer, but he's got an IT background that includes stints at NASA, the TSA, and the Navy. So he's got some pretty informed opinions about Security, Net Neutrality, and well, since he is an ops guy now—we do talk about cloud orchestration as well. That and more is yours in this episode of Cloud Unfiltered!

Niki Acosta: All right, good morning, good afternoon, good evening wherever you may be. This is Niki Acosta, and this is Cloud Unfiltered a Cisco video podcast, and I have a great guest with me today. This is Brandon Matheson. Brandon-

Branson Matheson: Hi.

Niki Acosta: ... tell us about you.

Branson Matheson: I am one of the lead technical engineers for the Cisco Cloud group, and I did work in the operations team dealing with day-to-day stuff as well as developing tools to make operations more efficient.

Niki Acosta: And you've had a crazy, amazing past. You sent over your LinkedIn prior to this, and we haven't really interacted that much despite working on the same product lines and the same business unit. I was checking out your LinkedIn and I was like "wow", and I saw security clearance and you know, you do a bunch of talks and there's all kinds of interesting things there so give us a little history about you and take this back to what you were like as a kid all the way up through today?

Branson Matheson: Oh boy. Okay. So when I was very young, I've always been into hacking, and when I say hacking the idea is to make something do something it was never intended to do, it's not necessarily malicious. And when I was I young I might have hacked the cable box in our house so we could get HBO and my mom called the cable company up and had them come out and was expecting them to blister me for hacking the cable box. The guy actually offered me a job because he said "You did something nobody else could ever do."

So I started that. I was in the Navy, I did cryptology as a cryptotech in the Navy. From there I went and worked at NASA on hardware. Everything from Cray, to SCI, to IBM, to a lot of deck equipment, broke my teeth in on BMS, if you guys can remember that.

From there I got a friend of mine who gave me a UNIX account for the first time and I started to learn UNIX and the rest is as they say history.

From there I was hired as a junior admin, within a year I had 200 machines under my belt, and from there I've worked various for large distributed plumbing companies. I did some work for the TSA. I did some work for the Department of Energy. I was the Director of IT and then the CIO for Silent Circle Blackphone for a little while. And then I ended up here and I'm working for Cisco and it's fun because they bring me the hard problems which is what I like. I don't like to have easy stuff to do, I like to have difficult things that challenge me and this job is definitely that.

Niki Acosta: Do you find yourself getting bored if you're not challenged?

Branson Matheson: Yes. Absolutely. My tagline is "I bet you can't make 'X' work with 'Y' and I bet you I will find a way to do it", it's just one of the things that I like to do. In my personal life I do crazy things like build lighting for the band I play in out of open source software. I teach classes on Raspberry Pi using cheap routers. All kinds of fun stuff. I always like to just challenge myself to do something bigger and better and different.

So yes.

Niki Acosta: What do you play in the band? Just out of curiosity.

Branson Matheson: I play bass, keys, and pedalboards. So I have a set of pedalboards that I play, if you're a Rush fan my idol is Geddy Lee and that was his style so I take a lot of his cues. I actually had a gig last night, was a lot of fun.

Niki Acosta: Renaissance man, you look like you're in good shape for having a gig last night by the way. For those who are listening you can't see him but he looks awake.

So I was kind keying in on the Black Circle work that you did. I also saw that you had a pretty high level of security clearance, obviously if you worked for the TSA and others you probably had to go through all that, but given that ... First of all tell people what Black Circle does?

Branson Matheson: Blackphone.

Niki Acosta: Blackphone.

Branson Matheson: So Blackphone was a subdivision of Silent Circle and Silent Circle is a company that solved software that was privacy enhanced communications and the Blackphone was going to be a trusted platform to run those tools on where you could then feel like your communications would be 100% secure.

If you run, lets say Whisper, or you run Telegram, or you run Signal or any of these other tools on an iPhone or an Android phone, while your communications may be secure, the platform you're running on may or may not be and so the idea was to build a platform that would be more secure and couldn't be intercepted before it actually got into the software.

So that work was a lot of fun and I was there for the first Blackphone and helped them get the second Blackphone out of the gate, and we had a lot of interesting customers as you might imagine, governments, and agencies, and so forth and so on. But the idea of communities and individuals particularly wanting privacy was really strong. I teach a hacking conference called Shmoocon every January and that's where I got to know the

people at Silent Circle Blackphone, and of course there is a huge number of people that are privacy focused, that care that their information remains their information, that it's not given out arbitrarily, or it's not requested arbitrarily, and so forth and so on.

So the idea of that as a job really appealed to me when it came around. They actually talked me into leaving NASA to go do that and I really enjoyed, it was a good time. I'm always looking to see what the next big thing is going to be in tech along those lines and given where everything is going on and everything is happening with information leakage and information control and so forth and so on, I think we're going to see more and more of those types of services either come and go, or come and be strong.

And it'll be interesting to see how they survive, or if they survive.

Niki Acosta: So based what is going on, how hard is it going to be, let's say, find someone who may have posted leaked photos of the bombing in Germany, or in Manchester? You know, they're pretty mad at us, other countries are pretty mad, but what does that look like as a security professional such as yourself?

Branson Matheson: So it depends on the quality of the person that did it right? One of the things that's happened with security is that its become a lot easier for just anybody to be fairly competent and fairly effective in doing malicious things using tools that exist.

So when you're taking about an information leak like that, let's say, these images or whatever, for them to distribute them if they're using even relatively easy to use tools such as maybe Signal, or Telegram, or some of these other tools that you can get on a phone, or their routing them through TOR using HushMail, or other tools such as that, it becomes very very difficult to track them down. I'm not going to say impossible because I am absolutely sure there are entities that are watching traffic in ways we haven't figured out yet, and so I believe that the capacity exists for people to be found, the interesting problem that they have is if they found them they don't want to divulge how they found them therefore it may not be culpable in court.

And that whole scenario just played itself out where somebody was, sadly, was peddling pictures on the net that shouldn't have been peddled, and they caught them, and they caught him using a means that they didn't want to disclose so they had to drop the case.

And so those kinds of things happen and I feel like that balance is going to be an interesting thing to watch over the next many years because I think the capacities and capabilities of people both watching the content and the people trying to sneak through the content are advancing rapidly so it's almost a game of cat and mouse.

Or even in trying to fight a virus right? We make one vaccine for it and the virus evolves and becomes something else that that vaccine won't do, and it's the same thing with vulnerabilities on the net where you have worms running around.

So I think, wholeheartedly, trying to find somebody that even use a modicum of privacy knowledge to obfuscate their communications it raises the bar significantly it almost governmental entities to be able to ferret them out that have just vast amounts of money to throw at that kind of a problem where they can look at ...

Niki Acosta: Which is what happened today right? I think I just saw [inaudible 00:08:19] phone that said there's been an ask of the Justice Department to go and find the leakers?

Branson Matheson: Right. Yep. And it will be interesting to see if they can. I'm not saying that it's not possible. Usually the problem doesn't happen at the technology level, the problem happens after the technology level. It's much easier to find ... The old saying is "Two

people can't keep a secret, one person can." Because if two people shared it somebody else is going to hear it, or there's some means of communication that can be intercepted to determine what that secret was.

Plus there's also this idea of metadata where, let's say, those pictures were transmitted across the net at a particular time, you can look heuristically at the data flows on the net and try to back trace to where that data came from and so you can do that without actually knowing what the content was, but knowing that the transmission happened at a particular time to a particular place.

Niki Acosta: Wow.

Branson Matheson: I think those capabilities are becoming bigger and bigger and bigger, and that would be the facility that's in Utah that the NSA had built would be a good example of information collection of that kind of metadata where they would be able to use it.

Niki Acosta: I do remember a few years ago there was a really awesome guy who joined the OpenStack foundation to do a keynote and he was from the NSA and he did his whole keynote and it was all redacted, he's like "So, you know I'm here. Guess how many servers we run?" It was like black bars on everything.

Branson Matheson: Yeah. Sure.

Niki Acosta: And later on we did a promotion for a deck of cards for people of OpenStack and he made the cut and I got really nervous when someone from the NSA called and said "You need to call me back." I was like "What is this about?" And she just wanted to make sure that we weren't profiting.

Branson Matheson: That's right, it's under $25.00 and all that stuff.

Niki Acosta: Yeah. There was like a whole thing about it. I was like "No, this is like an award." And she was like "Oh, okay."

But yeah it was pretty interesting to go through that process and just see how serious they are about security. Personally if I worked for an entity the NSA or anyone dealing with sensitive information I think I would be personally concerned that someone might be looking at my stuff all the time.

Branson Matheson: Well yeah, and having had a clearance they teach you to be circumspect about how you operate, what you do. I mean we walk out of the building and immediately put our badge in our pocket, it would be to that level, and you're very circumspect in all efforts that you are trying to achieve because of that. Whether it's who you're talking to sitting in a park, or you're doing work, or you're writing an email, it's all along those lines.

And I think those entities, for good or for ill right, I have personal opinions, but for good or for ill they've had some fairly major leaks. The latest Wanna Cry vulnerability that just ran around happened because the NSA vulnerability that they exploited and didn't report were found, leaked to the net, someone figured out how to weaponize it and then turned it around into Wanna Cry.

And so those things make them: A, look bad because they didn't release them, B, look bad because they had the leak, and so you want to not mitigate as much as possible your ... What's the word here? How you look to other people. Your ... I can't remember the word. I'm drawing a blank here. But that is almost as important as your credibility because if people start to lose faith in your capacity to perform your job well, or lose faith that you're a credible source of information then they're not going to rely on you as much and you're not going to be as effective.

So James Clapper and some of the ones that have been just railing about the leaks and the problems that have been occurring between Edward Snowden, and Wikileaks, with Assange, whatever his name is.

Niki Acosta: Julian Assange? Yeah.

Branson Matheson: Yeah Julian Assange. All those things I think have been very very impactful to the security apparatus across the world, not just us, but everywhere. And there are other examples, I don't want to go into them here, but there are other examples where its been very public, someone has given out information publicly that really probably shouldn't have and its been pointed out in the news that that was not appropriate.

Niki Acosta: Say no more friend. I'm with you. I got you.

So along those same lines I wanted to get your thoughts on Net Neutrality. This is something that's been in the news, you know, people who are in tech circles obviously follow it, people who may not be in tech circles may not even know what Net Neutrality is or kind of what the premise is behind it.

So give us a rundown on your thoughts about how you think about Net Neutrality and what the impact could be for some of the latest rulings that are happening?

Branson Matheson: So Net Neutrality is the idea that information that is flowing from one provider to another, or through a particular provider, can't be constrained by that provider arbitrarily. In other words if I am at home sitting and watching Netflix and I'm on Comcast or Cox or whoever I'm on, and they have a competing service they can't downgrade Netflix to make their service more attractive.

Which is one aspect of it, there are a lot of others that go into it, but it's interesting in having grown up watching the internet grow, peering points between providers has always been an issue of concern because sometimes you'll see them bandwidth constrain a particular provider and open up another one and usually there's money changing hands for that.

That is kind of what drove us to this idea of Net Neutrality and that said "Hey, hey. You can't do that, you've got to make a level playing field." And what that's allowed is small individual companies to be able to compete with large, huge companies and do the things they want to do without feeling like because they're a small company trying to compete with a big company their network traffic is going to be less and therefore their not going to get as much sales, therefore they're not going to be as successful, therefore they may as well part.

So, there's that aspect of it too, and then there's also the information control act where people who are sharing information on the net have some innate idea that their information will be free and that nobody can control the access to it or control the content, and that I think is changing. Its certainly changed for some of the more stricter countries like North Korea, and China, and even the UK and some of these other ones where they have put controls in place that say "Hey, you can't do that." Or even France that said "Hey, you can delete your profile on Facebook and nobody can ever find it again."

So globalization of the internet has kind of impacted this as well, but the problem becomes that if you have information that you want to share and somebody decides at some level that they don't want you to share it, especially if they're a government or a corporate entity that has control of those flows, then you can be restricted. So in this country we have free speech and that's very important to us, and these new rulings that

are starting to come down where individual companies, could restrict access to certain sites, let's say, it's an anti-Net Neutrality website, then they're using their corporate power to control their speech that is against their will, if you will, and they're doing it in a way that could snowball very, very quickly.

You also have the idea that with Net Neutrality information is free and information is not massaged, let's say, so if you are on a particular website and you get advertisements or you could information off this website the information provider that you have, the ISP that you have can not intercept your communications and change it as it's inbound to you.

And so now you have a much more interesting controlled environment where somebody not you, and not somebody you would trust, whether it's a government or a commercial entity, can now control what you see and what you think and I think as somebody who teaches social engineering this would be a classic case of controlling the narrative and if that persists we're going to have more trolls than we do now, and we're going to have more sheeple, as the term may go, because they're only going to get one point of view and I think that you can not be effective as an arbiter of control if you're going to vote, if you're going to participate in your government, if you're going to participate in the control of your own information, unless you are fully informed you can not do that.

And so Net Neutrality I think it has implications across the board. It's a very broad and scary topic, and it's interesting to me, I saw something the other day where apparently there 23 million comments on the anti-Net Neutrality thing on the FCC website and they're still moving ahead with it.

They also said they were DDoS'd and when somebody said "Okay, show us the traffic" and they said "Oh well, it happened" and they couldn't prove it.

So I think there's a lot of interesting things going on. Certainly I think the press is playing into this in both directions. You see some of the more open press, and certainly the press outside this country, being a little more anti-Net Neutrality and you see some of the press that's in this country that is associated with the major vendors that are looking for Net Neutrality to exist, say NBC, are being less anti-Net Neutrality, they are being more pro.

So again I think it has an impact across the board and I think it will, change our lives is an awfully broad statement, but I think as we're moving forward in this exploding capacity for technology to impact our lives the more that we allow outside people with disparate ideas to control what we see and what we think, we're going to have less opinion to be able to give that will be correct.

If you don't know all the facts and you only know some of the facts then you can't be an arbiter of truth. There's no way you can because you haven't examined all sides of the problem.

I know that was a long winded answer but I hope that-

Niki Acosta: No, that was great. And by the way I'm putting out on APB for anyone that is for it, if you have an opposing view I'd love to hear from you. Most definitely would like to get varied opinions on this show.

So switching gears a little bit, the reason why we initially started to do this podcast was around kind of your role in solving career problems and using Ansible and your career here and your experience in operating, and troubleshooting, and managing complex infrastructure.

So tell us a little bit about what Ansible is and tell us how it's helping you everyday?

Branson Matheson: Okay. So Ansible is what we call a configuration management system. When we talk about configuration management systems in wholes and what they impact we talk about machines and systems.

We talk about systems as cattle and pets, and so cattle are machines that you stand up, do something with, and slaughter. They're there for the duration of whatever need you have and you get rid of them, and that's very cloudy, if you will. And then pets are machines that you stand up, you nurture them, you feed them, you patch them, you make sure they stay up. They're long term viable systems that must be around for whatever reason, whether they're monolithic and can not expand, you know, they can't scale horizontally, you can have multiple of them and so if one dies you don't care, but they're that.

So the Cloud that we work in tends to be more cattle than pets, and for cattle you use tools that are more designed for what we call orchestration, where you're doing a step, and then another step, and another step, and another step. And those steps could be not just on one system, they could be on a diversity of systems, but all of the systems have to work together to perform a service.

And so Ansible is a neat tool that allows you to orchestrate. It certainly has its problems. Anybody that knows me knows that I will be happy to sit down with a beer and go through all the issues I have with Ansible.

Niki Acosta: Something tells me with problems every tool though.

Branson Matheson: Yes and no. I tend to look at things with a critical eye, and I tend to also believe in the right tool for the right job. So from an orchestration and an operations point of view I think Ansible is a great tool for those things.

In our particular environment Ansible is used to both deploy and manage systems and so we have built into it configuration that talks about all the systems that are there, the accesses to them, the controls that are too them, and so that was designed to able to deploy and manage the systems. Well it's great in that those exact same tools make working operations far easier because all the data is there. You don't have to have a list of passwords and go refer to it for every single host, it's already configured into the system to be able to go use. You don't have to go figure out which hosts do what, you don't have to figure out what roles they have, all that information is already built into the inventory because it defined what built the system.

So doing things like, for instance, if you have a user ... I had a customer say "Hey, I've got to replace a memory chip in this machine." Normally there's a certain set of steps that we would go in a checklist to say "Okay we've got to remove it from the cluster, we've got to turn off its networking, we've got to get all the instances off of it." We've got to do all these things and then we can hand it off to the customer.

So instead of having that long checklist now I have one command that I run, which is Maintenance Repair, and I run that command and it goes and does all those things including removing it from our monitoring tool so that we don't get alerts in the middle of the night because the machine went down when they replaced the memory.

Similarly when the machine comes back and the customer says "Hey I'm done with it, you can turn it back on." I have one command to run that reverts all of those steps and gets the machine back operational.

And the big benefit there is several. One, speed. Now I'm working at the speed of the computer being able to run the commands versus me typing them. Big benefit. But the other one is, as a security person risk is near and dear to my heart, and so being able to remove risk from any operation is a great thing. Using Ansible, with tools such as this you can remove a lot of the risk because you're doing the steps every time the same way consistently. Every single time.

And it's nice because you can integrate it with other tools, for instance that example I just gave you, it also puts a note in the ticket of the request saying "Hey, we've done this work to the machine here's all the data that we had to accomplish to get that done."

Similarly when it's done it puts a note back in the ticket saying "Hey, we have reverted all these steps and the systems finished. It's ready to go."

So Ansible really lends itself well to an operations environment because operations you almost always are doing steps, first of all, on multiple machines to deal with one service. So for that service I just talked about you'd have to go to the controller and tell it to remove it, you'd have to go to the monitoring system and tell it to not monitor it, you'd have to go to the networking system and say "Hey the networking for this instance is going to be down." All these different pieces and so Ansible really works well for that and there are a million other things that you can do with it.

Ansible, it's written mostly in YAML, which is Yet Another Markup Language, which is a fairly easy thing to write. It has it's origins in PERL, and PERL's big thing was there's more than one way to do it so YAML is written with that in mind and it's a very open and free flowing language. There's several different ways to represent the same data and so it makes it easy to customize and edit it. You don't have to know a huge amount of programming language to do it.

That being said, Ansible's language, such as if I can use that word, is not as well structured as I would see in other tools, which are the tools we would use with pets, and those are what we would call stateful tools. And those would be tools like Puppet, Salt, Chef where you define a state in configuration and then it applies that state to the machine. If the machine, something small changes with the machine, the tool will recognize that one thing has changed and revert it back to what it needs to be and deal with all of the dependencies.

The difference between that and Ansible is, Ansible doesn't really have a great dependency system. It just does everything step, by step, by step. So it's really good for doing an install. If you want to install something you're going to have a list of things you got to do, go apply it, great. And it's good for orchestration because if you have a process you have to execute, you have a list of steps you have to do, go do them, that's fantastic.

So that's kind of the rundown of Ansible. We've been using it in operations now for a while and its gotten to the point where I think it needs broader approach. I think more people need to start looking at this and so I'm going to bring this up USENIX this year, I'm going to teach a small class, I hope, on Ansible for operations one way or the other, and I'm certainly going to, on the hallway track as we call it where you sit around with your other peers in the hallway and discuss new things and better ways to do stuff, this is a topic that I definitely want to bring up and see how many other people are really looking at it from this point of view.

Niki Acosta: I love the desire to go out and just makes things better and that's one big thing I can say about communities is you get this feedback, you know, these hallway conversations and you can contribute back and make something better and that to me is so awesome. I wish it applied in every field, you know, just think about how far medical research would

be, or pharmaceutical research would be, or really anything if folks really collaborated and took an open source view.

That said, there probably wouldn't be as much money in certain things.

Branson Matheson: Well I think open source has lent itself to that. It goes all the way back to Richard Stallman and the GNU license, I think the idea that "this software is free, all you have to do is include this and you can build it, you can copy it, you can do what you want" that mentality has lent itself very well.

I was a free BSD developer back in the day and I watched a lot of the early communities come along as different projects came and went on the Net, and the one factor that I do note is that outside of sometimes you always get the rockstar that wants at the front of the crowd, outside of those very rare people honestly in this community you see a lot of people that really have just a strong interest to make things better and strong interests to improve.

How we do it might be a subject for discussion that doesn't come to fisticuffs, but beer poured on somebodies head is probably not unrealistic, but outside of that I think the desire to work together is an important one that we see in our community very strongly. It happens in the security community, it happens in the sysadmin community, it happens in the engineering community, I think. What I would like to see more of is those three communities, particularly, have more integration that work together side by side more distinctly.

The DevOps moniker has been applied to some of that, but I think you're going to have to see more and more of it because the pace of change outside of things we can control is happening quicker, and quicker, and quicker between vulnerability management, between hardware, between the ideas of virtualization.

You know, when I started out the big thing was clustering right? That was Dec VMS and that was Novell Networks, you clustered them. And then you had Windows come along and everything was monolithic for a while and they had central servers. And then you had thin clients, so you now you had thin little desktops and big servers somewhere running all this stuff and that kind of came and went. And now we're into the Cloud, and that's become a big thing. And now we're on the cusp of starting to see microservices and other things like that that are starting to be enveloped.

And so to their credit, most things like OpenStack, Cisco, even VMware and some of the companies like that are starting to embrace the idea that anything should be able to run anywhere, we just need to find a way to do it effectively. So whether it's running on bare-metal, whether it's running in a microservice, whether it's running in a whole server, whether it's running virtualized across many servers, however you want to do it, I think the pace of change is increasing and so for us to keep up effectively I think we, the arbiters of managing that change internally, you know, being able to both absorb it and then deploy it, will also have to be able to move faster.

So automation is the key. And so coming back full circle, Ansible, Puppet, all those tools that automate process that we used to do by hand for hours, and hours, and hours we can now do at the push of a button almost literally, I think those are the keys and those are going to continue to be the keys to the success of both the Cloud and general technology.

It's a little scary in that I think it's creating the premise that jobs are going to be phased out.

Niki Acosta: I was just going to ask you about that. I was interested if you thought it was a valid concern?

Branson Matheson: Yeah, and I think it's a valid one to a point. So the idea that jobs will be phased out ...

We had this discussion at a group I belong to at USENIX, and there's always going to be a need for the desktop manager in a small office. That's always going to be there. It's never going to go away. You know, companies like Google will say "Oh use our Google Office." And that's going to be effective to a point, but I don't think that you're ever going to see that go away totally. I think it's going to take a long time before that happens.

And same thing with tech support, desktop support, troubleshooting. I think system administration as an art that we have today is rapidly evolving into a DevOps developer type situation where you're automating most everything that you do and I would expect that trend to continue. I think the only place you're going to see sys admins as we have them now is legacy equipment and places like college campuses and others that have a fairly ... What's a good word here?

Even at NASA we had the same thing. In an academic environment you tend to have a broader requirement for different types of systems and different types of configurations and so forth and so on that can't be duplicated or replicated in the Cloud.

So for instance when I was at NASA, even recently, we had Windows XP machines. I had to manage 600 of them in "Windows environment" to be able to run software. We had testing apparatus that ran on Windows 98 that we could not get rid of. We couldn't put it on the network right? Because it would get owned in short order, but I think those types of environments you're always going to have a need for the unique people to be able to deal with the aspects of those systems that are not found in, you know, a Cloud, that are not found in a cluster, that are not found in a business.

A business can constrain very easily and say "Hey, we're only going to run Windows." Or "We're only going to run Mac OS." A business can constrain and say "Hey, we're only going to store stuff in DropBox. We're only going to use Zoom for our, or WebEx, for our communication." And that's easy to do. But when you're talking about academic environments like NASA, Department of Energy, and some of the other places I've worked you can't do that. That's not going to happen.

And so there will always be a need for those people there. Always.

Niki Acosta: My sister, it reminds me I have an identical twin so if anyone ever sees me and you say "Hi" to me and I don't say "Hi" back it's probably because that's not me.

But my twin sister is an expert at running teleprompters and there's not a huge market for the software that these teleprompter companies makes, but it only runs on old Windows machines.

Branson Matheson: Right.

Niki Acosta: So we had to get her a laptop and install a virtual desktop so that she could run this ancient technology, which works with all the still operating teleprompters that are out there in the world. Not a huge market for them.

Branson Matheson: Right.

Niki Acosta: So I see what you're saying there and I could definitely see a need for it.

One last question, and this is something I like to ask all my guests, but one thing that I do see a lot of is this desire to address problems, business problems, productivity problems, all kinds of problems, with technology. How important is culture in relationship to technology when solving these problems? Team dynamics, social dynamics, all of it.

Branson Matheson: Right. So it's interesting you mention that. USENIX which I've been part of the organization now for a while, we have a whole track on culture. That's all it's about. And we talk about culture a lot because, again as I said earlier, I think the open source movement, and the Unix world, and the systems engineering world, and the system administration world, whether it's Windows doesn't matter, I think it's engendered a very strong culture of people and it's interesting having watched the different types of people that get involved in that culture. You see the very quiet people, you see the beards in the closets, you see people who are very outgoing sometimes, you see some incredibly smart people, and it's a very diverse organization of groups of people, but what you do see is they all have a common theme and thread.

So it's interesting, you were asking earlier, I still am on IRC and I still find a lot of the best conversation about systems and engineering, and how to deal with managers, how to deal with customers, how to best approach a problem, you still find those communities out there even in IRC, which is its been around since the early 90s?

I think you're going to see that you've seen some people adopt the book of faces, and you've seen some people adopt Google Plus, and some of these other things, but the technology communities are still, outside of things like Stack Exchange, which I think has done phenomenal work along those lines, you still see them in niche places. You don't see them clustered together in large groups. And I think it's one of the interesting things that a lot of businesses struggle with is trying to tap that culture. Trying to find ways to effect that culture. You know, I've seen different companies use different approaches in trying to do it and it's difficult because they almost spring up organically based on the group of people, based on the locale, based on the common work.

In my role I end up working with people in the morning from Europe, and in the afternoon from California so I get a very broad spectrum of ideas, and thoughts, and diversity but it's interesting in that a lot of the impetus to improve things, as you were asking earlier, that is pervasive. You don't see that not exist in our groups.

Now I think it probably has a lot to be said that we have an extremely intelligent group, which is really nice. It's great to work with your peers. Its fantastic to be able to work with your peers like that. So the expectation is you would. You would see people step out of the box, think differently, find good solutions, and try to apply them and do it in a group format.

But even then in other places that I've worked, whether it was NASA, whether it was some of the other places you still find good collections of people that kind of congregate and form these little communities to be able to come together and solve problems.

One of the things I did at NASA was, I tried this once myself, so I created sysadmin.nasa.gov which was a website for all of NASA. IF you look it up on YouTube I have a nice little cheesy video I made one day about it. The idea was to build a community and a place for people to come together and try to share information. Whether it was how to fix a problem, whether it was a unique full script, and it worked sort of, but the thing that I found was that niche groups whether they were at Ames, or Goddard, or Lewis, or any of the other sites that we had they had their own little communities and it was hard to try to bring everybody together.

We did have an IRC that was NASA wide, if you will, and we had individuals from different centers on there all the time and so I got to know a lot of the people across there, but even within those centers those people were part of a community in their center, and then they were a part of a community with us, but there was never a shared community.

Niki Acosta: You think companies are doing enough to facilitate the culture change necessary to take advantage of the latest and greatest technologies?

Branson Matheson: It's not that I don't think they're doing enough, and believe me I'm certainly not the one to ask on how to do this, but I think nobody has figured it out yet very well. I think a lot of companies have come a long way from where we were. Used to be we all had to do this on our own, which is why IRC came around, which is why Wiki's came around. It's because we got sick of just writing text files on a share somewhere and started trying to find ways to organize our information better.

So I think companies are starting to give us tools to do that that work a lot better than what we have had before, but as far as taking that from just a community to a whole culture, raising the bar as you will, it's a hard step to make.

The closest company I've seen, from what I've heard, to get there is companies like Google and companies like SpaceX who have ...

Niki Acosta: Who weren't founded that long ago.

Branson Matheson: Right.

Niki Acosta: Generally speaking in terms of the enterprise, they're kind of newer kids on the block right?

Branson Matheson: They are and think that the big thing here is that they were able to get like minded people in quickly and because of that they were all organized together, whereas most of the other companies I was talking about, whether it's TSA, NASA, or the rest of them, they've been around for a long time and they weren't necessarily ... Well NASA's where I got on the internet for the first time back in the late 80s so I mean it's been around for a long time, but at the same time they didn't organize into a community that was across the board.

And some cultures, one of the things that they said Columbia failed, or the reason that Columbia failed was the culture of safety, that was at NASA there's a whole report on that that you can read, it's worth doing. But some culture building hasn't gone well, and that would be I think a good example of it where they started letting things slide to get to a goal and so when they said "Hey, we need to look at the under side of the orbiter" and upper management said "No you don't need to do that" and then it came down and there was a hole over near the landing gear. We had a failure and I think that's a concern.

And I don't see that in a lot of corporations. The thing I see in corporations is usually either customer or money driven. The best corporations I've seen are customer driven, by far. The ones that are they will make the changes for the customer, they will go out of the way for the customer, that usually leads to the money. The worst corporations that I've seen are the ones that look at the bottom line and make their decisions based on that, and usually, unfortunately, a lot of small companies end up in that pocket because that's all they have. They don't have a customer base that they can improve upon and then build money from it, if you will.

Niki Acosta:	Excellent perspective. Well Branson we are about out of time. I don't know if your rain storm is going to prevent you from coaching that soccer game tonight.
Branson Matheson:	I don't know, we'll see.
Niki Acosta:	But I wish the best of luck on that. Where can people find you if they want to get ahold of you?
Branson Matheson:	So anybody that wants to find me I'm on Twitter @Sandinak, if you want to know what that is ask me, I'll tell you, it's kind of a funny story. I'm on Fnet as Sandinak, I hang out on the League of Profession Sys Admins channel, LAPSA. I'm almost always there. Of course at Cisco, if you're at Cisco, I'm BrMatheson in the directory and you can find me there.
Niki Acosta:	There was no eye roll there I promise. For those of you just listening and not watching there was no eye roll there. So there. Well I'm glad you're on our team because you're really smart, and I look forward hopefully to seeing you out and about. I know you speak at conferences and you do lots of cool things and so I really, really, I know you're busy and I thank you for taking the time to speak with me today. Thank you Branson. Please subscribe to this, please leave your comments, please let us know who you want to hear on this video podcast, or see on this video podcast. We'd love to hear from you. That's all for today. Branson say bye!
Branson Matheson:	Bye. Thanks everybody. Have a great day.

For More Information

Find more Cisco Cloud Unfiltered podcasts.
Learn more about Cisco Cloud solutions.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA 05/17