Integrating Cybersecurity into IT Procurement: Insights from Montae Brockett and the Art of Hip-Hop in Tech

Speaker Names

Telice GillomHost

00:03

Welcome to another episode of the NASPO Pulse podcast. We're your go-to for riveting procurement conversation. I'm your host, Telice Gillom, and for today's episode, my co-host is Chadwick Stephens, NASPO's Research Manager. Chadwick, thanks so much for joining me.

Chadwick StephensCo-host

00:21

Hey, thanks for having me on Long-time listener, first-time caller.

Telice GillomHost

00:26

Chadwick, who's joining us today.

Chadwick StephensCo-host

00:27

Well, on today's episode, we're talking to Monte Brockett, cio and CISO from Washington DC's Department of Healthcare Finance. Monte will be talking to us about cybersecurity and risk mitigation.

Telice GillomHost

00:41

Now, you know, Monte is somewhat of a cybersecurity guru, so this is sure to be pretty exciting if you're a computer nerd, which I am.

Chadwick StephensCo-host

00:50

Hey, I'm not the most tech savvy person, but I do think it's valuable for our listeners in the procurement world to keep the conversation going about tech.

Telice GillomHost

00:59

You're right, technology is pretty inescapable and for procurement professionals in particular, it's a great idea to talk to your tech folks as much as possible. Monte also talks about strategies for bringing information security and IT fundamentals into the procurement process.

Chadwick StephensCo-host

01:16

So get ready to download some cybersecurity knowledge.

Telice GillomHost

01:19

And make sure your firewall is enabled. We appreciate you tuning in. Remember to subscribe to the NASPO Pulse podcast so you never miss an episode, and feel free to email us with your questions.

Chadwick StephensCo-host

01:30

And to the person who stole my license for MS office. I will find you. You have my word.

Telice GillomHost

01:36

Press any key to take the pulse, Monte. Thank you so much for joining us here on the NASPO Pulse podcast. How are you, my friend?

Montae BrockettGuest

01:45

I'm doing good. Thank you, Telice. How are you doing, Chadwick? I appreciate you all giving me the opportunity to sit here and talk to you all about cybersecurity and risk mitigations related to IT procurement. So, hello, how are you? My name is Montae Brockett. I'm currently the Deputy CIO and Chief Information Security Officer for the Department of

Healthcare Finance. I've been in the industry cybersecurity specifically for the past 14 years, you know, assisting multiple organizations from the public and the private sector.

Telice GillomHost

02:18

Sounds pretty good To have a CIO and CISO title. You must have lots of credentials, sir.

Montae BrockettGuest

02:25

Yeah, I have several different certifications. I'm going to give you a couple of them just for you all to know who you're speaking with my experience in the field and my expertise. I currently hold a certification in cybersecurity management and policy from the University of Maryland. I hold certifications from ATT&CK IQ and MITRE ATT&CK Framework applying world-class research for threat-informed defense. I have several certifications from CompTIA, specifically Security Plus and Network Plus. I heard IC2 certification to certify information security manager Also. I heard efficient expert security manager Also. I heard efficient expert. I've done security information event management. I heard Databricks analytics Also I have. I am a Palo Alto network instructor as well and I've been doing several other Azure and AWS certifications within the last month.

Chadwick StephensCo-host

03:24

So it sounds like we got a real expert with us today. Chadwick, what do you think? Absolutely Up to date on the latest, the greatest, he's naming?

Montae BrockettGuest

03:32

things I've not even heard of yet. Yeah, chad, thank you. Thank you, chad. Thank you, Telice. Yes, yes, I kind of am a steward of, just you know, looking at the new technologies, trying to align my knowledge with that so I can support the organization's mission and vision and, with that being said, just being able to participate on, within the last couple of years, about 15 different panels across state and local cybersecurity summits, talking to other cybersecurity leaders, looking at the rapidly evolving threat landscape and also how organizations hire and retain the top IT security talent.

Telice GillomHost

04:08

That's amazing. So you know, october is Cybersecurity Month and many of our NASPO members really struggle with IT projects for a variety of reasons and, you know, due to those struggles sometimes they can be less familiar with their agency's cybersecurity needs. From a CIO standpoint, tell us about your process for getting your procurement, your IT and your cybersecurity staff in sync to get your agency's needs addressed for IT projects.

Montae BrockettGuest

04:40

Okay, I guess you know I've been here at Department of Healthcare Finance in DC, which is the healthcare agency for the District of Columbia, and I've been supporting the CIO as a deputy CIO but leading the charge as the chief information security officer. And one of the most important things, when you know, sitting in this role is being able to understand the mission and vision of our organization and being able to align technology procurement and contracts to that mission and vision. So it takes understanding and documenting and defining the strategy for the next three to four years as it pertains to achieving those outcomes for those specific administrations within our organization. So I think the most important thing is just being able to strategize, using your team members, bringing them together, understanding what those needs are, discussing and having meetings with your administration, stakeholders, directors and senior level managers and just letting them discuss what their biggest needs are and how we can address those needs with technology or business process automation.

Chadwick StephensCo-host

05:48

So, monte, speak to me from a CISO standpoint. That's, a chief information security officer for the uninitiated. So, from a CISO standpoint, what would you say are your biggest challenges with those IT procurements?

Montae BrockettGuest

06:04

What would you say are your biggest challenges with those IT procurements? I think the biggest problem or challenge is that, from a CISO perspective, is, you know, the different knowledge that each function within a specific organization has. We are subject matter experts on technology and procurement are subject matter experts on how the

procurement process and contracting should go. Needs are from a vendor, while also ensuring that we meet the guidelines and templates that our OCP Office of Contract Procurement has in place as it pertains to what is needed to be able to get that statement of work out the door in that solicitation published.

06:59

And one of the things that I think we do well here at DHCF is work together. We collaborate a lot with our contractor procurement offices and sometimes it just means, you know, having five or 10 minutes of your day just to explain the technology, whereas it be, hey, what is SASE? What is a software as a service? What is a subscription as a service? Does this apply to this actual procurement process? What is a subscription as a service? Does this apply to this actual procurement process? It's one of the biggest things that you see in the gaps from a procurement process standpoint and it's important for technology leaders to kind of bridge that gap and work with those other functional areas so we can ultimately make sure that we are getting the vendors in here that actually can meet the actual needs of that administration.

Telice GillomHost

07:47

So when we talk about cybersecurity, you know we're also talking about risk management. Like you mentioned at the beginning. Risk mitigation and risk management kind of go hand in hand. And when you and I met earlier this year at a cybersecurity conference, I was very impressed with your description of your own unique process for third-party assessments. For suppliers that would be selling your agency software. You do a third-party assessment of them beyond the evaluation process and if you wouldn't mind, I would love it if you would give our listeners a brief description of that process. And I understand you can't go into too deep details, but if you could just give a synopsis of what you do, that'd be great.

Montae BrockettGuest

08:32

OK, thank you, Thank you. Thank you, talese, appreciate that. So, yeah, just like you said, without going into a lot of details on how we accomplish this review, think of your vendor as someone looking for credit Right. Think of your vendor as someone looking for credit right, and it's your obligation as a creditor to ensure that the vendor meets certain standards before engraging in business with this organization.

09:05

Information is critical to make sound decisions about a person or organization's ability to provide the services and have the ethics needed to extend business opportunities too. So I think of this as a digital credit where we establish risk rankings on the way they currently do business and measure that goes into the selection process. So, from an external perspective, there are many organizations right and I see you know with external threat, landscape management solutions or grand reputation solutions. Most of the time, 70% of the organizations based off of their digital environment are meeting about a 70%. That means 7 out of 10,. As far as risk score, when we talk about public-facing resources right, and that's things that are directly interfacing with customers that information is used. Basically, the risk score is used to be able to determine the amount of risk the organization is willing to take right, and that's how we establish our risk mitigation and think about bringing all vendors to inside of our environment.

Telice GillomHost

09:58

You mentioned a risk score. How often do suppliers get a passing score? What is a passing score for your assessment and how often does that happen?

Montae BrockettGuest

10:08

Well, most people look at risk scores between one to ten. Right, and when we think of it, you know you have a lot of things. That is informational. Some things are critical, some things are high, some things are moderate. Things are moderate when we talk about risk classifications.

10:28

I think when we talk about it, we look at anything from a seven to above is highly risky, right. And we're talking about domain name services. Basically, people spoofing your domain name Say this is googlecom, but I want to say googlecom with an I on the end. It's basically taking that brand reputation, using it, you know, creating this digital presence or profile as a bad threat actor and, you know, using that to be able to exploit vulnerable customers. And when we look at it from our standpoint, we just want to be in a position where we can help our partners that we do business with. So it's not ultimately to say, ok, well, I don't want to do business with you because you have a 907. But how can we work together to take this score to an acceptable rating that can actually meet our risk tolerance from an organizational standpoint?

11:28

Because if you follow the risk management framework, you have three levels. You have organizational risk, you have the mission and function risk, and you have the IT systems risk. Being able to collaborate and aggregate that data and use analytics to provide information provides you the context to make sound decisions as it pertains to vendor selection. So these are some of the things that we use. We don't, you know, say okay, well, just because you have a nine or 10, we're not going to do businesses. Sometimes you're a leader in that sector, right, and sometimes you just can't do it without the product or service. So you're going to be faced with multiple different decisions. But lean on your partners. Do that brand reputation, do that digital review, you know. Invest in external threat landscape management platform. That can help kind of surface that information. That is going to be critical for you to make the decision when it comes to onboarding or being a partner with any type of organization Right.

Chadwick StephensCo-host

12:31

So what are some of the reasons that these providers don't pass your security assessment, like what are some of the most common vulnerabilities that you see?

Montae BrockettGuest

12:39

I think some of the most common ones are being identified on the Common Vulnerability Enumeration List, the CVEs. Right, you can look at some of the known vulnerabilities that are impacting systems across the world. Right, it has been, you know, present in our environments for over decades and we still see organizations with these vulnerabilities, see organizations with these vulnerabilities, and that comes from, you know, not being able to deploy those patches, even not doing due diligence as it pertains to reducing those vulnerabilities, and just sometimes, they just don't know where the resource is at. We have a lot of things that's called technical debt, where we buy all of these products or services and, you know, we don't really use them. You know, we have one strategy in this fiscal year, but three years later, this actually technology sits on the shelf and we forget about it.

13:35

Think about cloud services now, right, it's so easy to spin up a virtual machine. It's so easy to spin up technology. These things are sometimes being left. It's like leaving your door open in your house. Right, if you leave your door open in your house, somebody is going to walk in, look around, peruse, see what type of data we have in there. If we have something

in there, we might take it right end when we look at IT and modernization and innovation is that cloud services is making things easier, but it's also making things more accessible.

Chadwick StephensCo-host

14:10

You said one of the magic words there modernization. So modernization is number one on NASPO's top 10 list of priorities for 2024. We actually had an hour-long webinar back in June talking about ways our members can modernize their procurement offices. In order to do the kind of processes that you've been talking about, you must have quite a modern digital environment in your office as well.

Montae BrockettGuest

14:35

Well, I would say we do have a, you know, improving digital environment, like most organizations, but I think it's far beyond the technology modernization. I think it's more focused on business process modernization, focused on bringing our user community where our technology is today, because they are always the critical point. Where, though, they're always so far behind, where technology is continuing to be driven, continuing to innovate. We're going to continue to modernize, right, so, being able to take our workforce, educate them, you know, bring them with the technology I AI, and being able to support topic at the cybersecurity conference that we attended.

Telice GillomHost

15:41

What would be your strategy to fill those roles? How do you train people to fill them?

Montae BrockettGuest

15:47

We have to be intentional in the cybersecurity community and the IT community. We have to be intentional. It's important that we look at the digital community, right, and we actually, you know, get on the front lines. We start to, you know, ensuring that these major technology companies come closer to the communities, providing these free resources, providing these virtual labs, providing the context that these individuals need to be able to understand what enterprise operations look like.

16:22

You know, one of the problems that we see, that I see in my opinion, is that we have, you know, I'm a component of open source products, right, but you know, when you work in real environments, open source products aren't used readily.

16:41

Right, and most of the organizations are using licensed commercial products and you're saying, ok, well, I want to bring this individual in, but the product that you use is a commercial product, is a commercial product, right, and they don't have the understanding because that product might be $50,000 to $40,000 just to actually use administrator.

17:05

The actual cost might be $7,000. So how do we ask these cybersecurity companies or these major technologies companies to say, hey, provide a virtual environment, provide them hands on, easy to use platform to educate themselves? I've been one of those individuals that normally I started in accounting and I changed my career several years ago into cybersecurity, using ComTee and TestOut as the learning platform to train myself without having formal training through a college participation. Once I understood the amount of resources that this platform provided to me, I was able to create me a new career path, which is cybersecurity where I'm at today, with 10 years of actual study and hands-on practices and activities and just going to a lot of conferences and putting me in a position to be able to help and reach back out to other practitioners in the field.

Chadwick StephensCo-host

18:13

So, of course, we couldn't talk about emerging technology without mentioning AI. It's one of those things we try to stress to our members and all of our listeners is that generative AI is already included in the products you use every day, and it'll probably be included in the goods and services you purchase on your agency's behalf. So give me your take on these AI-included products.

Montae BrockettGuest

18:45

It's hard. It's a hard topic to discuss because we're still all struggling with understanding and identifying those best practices. What are those processes? Are you know when we're talking about onboarding AI-type products?

19:03

I think one of the most important things that we need to do is embrace AI right, and not just from a technology standpoint, where it's baked into security products and security services, but use them in the OCP's aspect. Genitive AI can be used for chat box, answering real-time questions from IT professionals, reducing some of the stress on the contractor procurement offices by storing that information. That's important that people need to be answered. They not always have time for a contractor procurement professional to get on the phone, but if I had a chatbot to ask it a question, I might be able to get the answer to my question faster. You know, if I ask it for, develop me a template, it can do those things. Let it review a documentation for me, make edits, improve some of the things we do. It's how generative AI can support not only IT cybersecurity but also can improve the OCP and contractor procurement process in a massive way if we actually use it and implement it the right way.

Telice GillomHost

20:17

There's a lot of changing legislation, particularly around AI and procurement at the government level. Any of our members or any of our listeners who are interested in tracking those legislation changes. There is a newsletter that you can get via email called multistateai multistateai, and you'll get an email once a week. Maybe that will update you about the most recent legislation changes at every level of the government governmental agencies like DOD, the Department of Defense or other public agencies that are really taking a good look at what the policies need to be so that the procurement office can procure those AI-included products without worry of what does the procurement code say? What do our regulations say?

Montae BrockettGuest

21:21

Yes, that's important to Lisa. I think that's an important resource for us all. So I'm going to take that and jot that down and take it back to the office question, right?

Telice GillomHost

21:31

If you're listening now make a note.

Montae BrockettGuest

21:35

You better make a note.

Telice GillomHost

21:38

So another large pain point for our members when we start talking about IT procurement and cybersecurity are the contract terms and conditions that come with those projects. Put your CIO and your CISO hat on again Two hats at the same time. Yes, can you talk a little bit about your approach for your agency?

Montae BrockettGuest

22:01

I think my approach is, you know, understanding what we're trying to do, understanding what the administration is trying to achieve, ensuring that we define all of those requirements from the administration and then start to see how technology supports what those requirements are. When it comes to the terms and conditions that are definitely included into it. We have some standard language in like. Most states or federal government or any other organizations have those kind of standard languages in there. We have one that's called a business associates agreement, and that's one of our kind of living documents that HIPAA prescribes as it pertains to doing business with anyone.

22:50

So a lot of times where I see that issues comes where, though, when you have those authorized reseller scenarios where you have organizations that are providing the tech for you, but you have authorized resellers are the ones that are selling the tech. So who's accountable for the risks associated with the procurement of this product? And that is one of the biggest things how do we address those things? So my thing is make sure that you're clear with your general counsel, make sure can you accept the risk that is associated with any removal of any term and condition from a specific contract?

Telice GillomHost

23:50

healthcare finance. You have two very important sets of information or data to protect HIPAA information right of your constituents, but also the finance part, and so when we're talking about terms and conditions, there are some sticking points there for those. Do you run into issues with negotiating those terms and conditions? Knowing what you have to protect, you have to protect. You know personal health information, personally identifying

information and finance information for your constituents. Do you run into issues with negotiation of terms and conditions about that?

Montae BrockettGuest

24:38

run into issues with negotiation of terms and conditions about that.

24:42

I haven't had that many cases, to be honest.

24:48

I have had one case, most recently within the last year, where we had a major organization that kind of pushed back on signing one of those business associated agreements based on the implications of provisions that would have been on top of that organization.

25:04

I think when you look at those major companies and the amount of business they do across the globe, it's kind of hard to get them to change their business practices to meet the terms and conditions that you have set forth at a state or local government level. Right, and sometimes you know there's no resolve to that issue. And sometimes there is when it comes to a financial or fiduciary issue for that specific organization, to a financial fiduciary issue for that specific organization. So how we deal with it is, you know, we set forth what we expect from our vendors and if our vendors cannot meet what those expectations are, we have to move on to the next available contractor to ensure that we still produce the outcomes for our district residents. We are stewards of their information so it is of our utmost importance to safeguard that data at all costs. So we're doing things as it pertains to how we need to protect the data, what we think is the best safeguard that needs to be in place before allowing any organization to do business with it.

Chadwick StephensCo-host

26:31

So one of the things I think I've taken from this conversation is that with new technology comes new risk. Anytime you see the word new, you might as well think of the word risk. So, monte, how does DCHCF achieve a balanced, say cybersecurity landscape? Like using this new technology in a smart but safe way to provide the necessary services.

Montae BrockettGuest

27:01

Oh, so we use, like most organizations, we go through a risk management framework. We follow the seven steps in the life cycle to be able to prepare our organization. We assess the risks associated with any technology, then we ensure that the controls or the standard controls that are needed or our best practices that we employ, are implemented. You know we can do continuous monitoring. So I think, following that RMF process, it helps us identify the risk, it helps us make the decision as it pertains to what amount of risk that we can and cannot take. And I think all organizations mature in that. If you're just starting in, start at one system, start at one process, just start because it will help you greatly to be able to identify risk from the organization. And it's important for, from a cultural change, that senior leaderships adopt this risk management framework to be able to add value to the process and be able to add value to your decision making.

Telice GillomHost

28:10

When we were at the cybersecurity conference earlier this year, they talked about the likelihood of threat actors already being in a lot of agencies environments, sometimes due to lack of IT knowledge from staff, sometimes due to aging systems, and the federal government has adopted what they're calling a zero trust policy as a best practice. What's your take on that?

Montae BrockettGuest

28:39

I think you know zero trust is a buzzword. I think we've all been doing it for years now. I think you know the maturity of zero trust, of what they call it, needs to continue on, to build on top right. It's things that organizations need to do. You know that is first. You know, I think a lot of the products that we are currently procuring today are natively zero trust because we are moving from on-prem technology delivery to cloud services. You think about, you know this secure access service is SASE type of methodology, where you have Zscaler, all of these kind of products. Palo Alto provides those things, crowdstrike provides those things. A lot of these organizations are starting baking zero trust into them. So I think, organizational-wise and I know from my opinion, you know we have work to do and this is not something like it's just turnkey. A lot of preparation has to be put in place, you know, to be able to actually achieve what that zero trust maturity level is, or being set forth through OMB.

Telice GillomHost

29:57

And OMB is the Office of Management and Budget, and you're right, it is a buzzword that they use, but it is federal procurement that we're talking about. Everything is an acronym, everything has a term that doesn't mean anything outside of that context.

Montae BrockettGuest

30:17

Correct, correct, correct, correct. And I'll say, if it was simple, from in layman's terms, be able to verify every interaction with any sensitive system or data that you have. You know, that's what you would do at your house, that's what you would do if you was going in a club, that's what you do when you go to the bank account. You have to identify yourself prior to getting access to anything, right. And why not take that same kind of concept and move it into the technology, move it into your business process? Let's verify, let's validate before we just actually approve it right, before we just actually approve it right. And we should use that across the procurement process, the technology process and actually organizational level.

Chadwick StephensCo-host

31:05

Best case scenario. Cybersecurity is one of those crucial functions of any agency that kind of stays in the background until it doesn't right. Correct. Yeah, so I think we can remember this. Past July there was a worldwide outage from a security patch. So many companies airlines, banks, public agencies, cities, counties, public universities everybody affected. So did that affect your agency at all? You can put your CISO hat on again. I'm curious as to what your policies are for these Black Swan events.

Montae BrockettGuest

31:46

Yeah, so I think you know being prepared right. Incident response, business continuity, disaster recovery all of these things are something that we practice every single day. So any event, large or small, we should be prepared to respond to. Yes, we were impacted, not, as you know, a longest outage as most organizations did. I think our partner that was impacted did a great job in responding to it and assisting the customer to get all of our systems back on live so that we can provide the operations to our district residents as we normally would do. You know, with these events. It just highlights the importance for tabletop exercises

right To go through different events. You know bringing down your system, seeing how people operate right. So I think it really was a great thing that it happened.

32:48

I didn't want it to happen, it shouldn't have happened, but it was good to be able to see where organizations were from a cybersecurity preparedness standpoint and that it was crucial for us because we never had this. You had so many individuals saying this would never happen to me. This wouldn't happen to me, but when it happened to you, did you have the staff prepared? Did you have the technology in place? Were you able to continue operations? Did you have the technology in place, were you able to continue operations?

33:17

And we saw blindly that most organizations could not and was not able to recover in an acceptable timeframe to still provide services to their customers, which ultimately impacted what their financial obligations. Follow the money which goes into one the biggest thing our risk management framework. When we identify risk, we identify the impact and likelihood of that risk happening in your environment and what to do when it does happen. There was a lot to learn and you know I'm appreciative of it. I don't want to happen again, but I'm definitely appreciative of it and I think we all learn and I think the United States, globe and global customers, we all work together to get this back up and running.

Telice GillomHost

34:06

I think it kind of goes to show no one company should have that much reach into so many crucial industries throughout the world, many crucial industries throughout the world. It's not best practice Because if one company has an outage that can affect so many different types of industries and areas, of government. Somebody maybe should look at that a little closer.

Montae BrockettGuest

34:34

Yeah, we need competitors in the market and know and I think one of the biggest things that I've seen is this Gartner and Forrester that provide a lot of good context and ions that provide a good context on organization product to see what are comparable products. And you had so many conversations about, hey, should you have an additional security protection with the one that we just had or should we just get rid of that? We don't make

decisions like that. You can't make decisions like that because the actual disruption of operations is never acceptable. Right, and when you make drastic decisions when it comes to technology because of an event, you can actually hurt the organization more than improving it and making it better. Right. So work with your vendors.

35:25

You know, again, doing our due diligence in the procurement process to see what, what is their recovery time objective. You know these are things that need to be outlined in what, the terms and conditions. These are the information that we just gloss over when we talk about a procurement, an IT project that becomes important when the things actually happen. Who's liable for it? How did that cost being broken down? When should that cost be allocated to the specific impacted customer? These are all the questions that need to be addressed, but you don't know it until you actually go through it. And that's just life story.

Telice GillomHost

36:06

One of the things we love to do here at the Pulse podcast is tell dad jokes, because they're all so funny. Who doesn't love a good dad joke? So, gentlemen, I know you're both dads, I know you got some dad jokes for me.

Montae BrockettGuest

36:21

Yes, chad, you want to start out first. Yeah, yeah, you know what? I'll keep it topical.

Chadwick StephensCo-host

36:26

We've been talking a lot about cybersecurity. The Internet of Things keeps growing. I heard there's even now smart billboards, these billboards that can communicate with each other. Oh yeah, you know how billboards talk to other billboards, how Sign language? Yeah, that's good, listen, listen. I've been wanting to learn sign language. Seems like it'd be pretty handy, right, ah?

Telice GillomHost

36:56

I see what you did there Well played, sir. Thank you, thank you, thank you.

Montae BrockettGuest

37:00

Well, I would have a. I think I would have to say I don't have the best dad jokes. I think the dad I have jokes when my daughter has done. You know, like yesterday, I was sitting in a room and I was like, hey, turn your music on. And I didn sitting in a room and I was like, hey, turn your music on. And I forgot what type of box she had. And I just sat there and I kept saying, hey, alexa turn up. I said Alexa turn up. And I said Alexa turn up. I said I think about 15 times. I said this is broken. And then my daughter turned around and said, daddy, and she's four years old, I thought you should have been saying hey, google, daddy. So I forgot that we had the wrong thing. It was Google, it was a Google Home. So I sat there, I thought the thing was broken and my daughter sat there and watched me, I think for about 10 minutes just screaming at this thing like this is broke.

Telice GillomHost

37:57

She probably thinks dad's an old bogey who doesn't know what's going on in our cyber environment, in our home. Dad, why don't you know what type of smart home we have? You're the cyber guy, I'm sure she has no idea what cyber security is, but I'm certain in that moment she probably thought out of it.

Montae BrockettGuest

38:14

Yeah, and I'm just. She just sat there and watched me do it for 10 minutes and I'm just, I'm getting frustrated at this time because I'm like I'm ready to eat. So that was, that was my dad joke, funny from yesterday, and it's every day this young lady surprises me with a new joke that I got to deal with me, with a new joke that I got to deal with.

Telice GillomHost

38:36

So one of the things I also know about you, my friend, is that you're a big fan of old school hip hop, like us. Chadwick and I have a funny running joke about all the old school hip hop we talk about and the stuff that we listened to growing up and how different it is than the stuff that's out now. Yeah, we laugh about who's good, who's not, what we don't know about the current music scene, and that's a lot.

39:03

Yeah, some of it willingly, some of it most of it willingly, most of it willingly, because I have no idea what they're talking about, just like. It has its own language. So too does the current state of music. Genres aren't defined anymore, and there's a lexicon that I don't know what it is.

39:29

It's quite different than what we all grew up listening to One of the things that for our listeners and I'm sure maybe if you love old school hip hop too or you like old school music top five lists. So Chadwick and I joked and laughed about our top five lists and you don't have to do all five, you can say a top three if you want. But what are your favorite top five old school hip hop artists? What are?

Montae BrockettGuest

39:57

your favorite top five old school hip hop artists. So I went back and I did some research on it and I was thinking about all my new music and I didn't want to leave people out. So I said Tupac Shakur All Eyes On Me, you know, definitely was a resonated. Then I went to Drake, I went to Little New School and he had God's Plan. That was a good record. And then I just went way back and thinking about Dr Dre and I said straight out of Compton, right. Then I said, ok, well, it's cybersecurity month, you know. So I said Notorious, big Warning. We're giving you our warning. Great choice, quite topical, very, very topical. And then I finished it off with Jay-Z, the Empire State of Mass, right.

Telice GillomHost

40:46

Nice.

Montae BrockettGuest

40:47

And that topped out my hip hop top five, and I think those songs resonate with me every single day as I, you know, matriculate through this IT space.

Telice GillomHost

40:57

I love it. We really appreciate you taking time to talk with us today. We really learned a lot. Definitely, what do you think, chadwick?

Chadwick StephensCo-host

41:07

Yeah, no one's ever called me a tech person, and you were able to explain this in ways that even I could understand, and I'm very appreciative of that.

Montae BrockettGuest

41:18

Matt. I thank you Talisa, Thank you Jarek and Nazbo. Definitely, you know this was a great conversation. It was important to get this information out there and, you know, ensuring that. You know we all understand that collectively we can move the needle in the technology space, speed up procurement process. Ultimately, I know that what the readers want to do but understand that your IT professionals, your security professionals, are there to help and support you Right, build the relationship, maintain the relationship relationship, maintain a relationship, stay in close connection and work with each other to be able to achieve the goals of your organization.

Telice GillomHost

42:04

Well said, gentlemen, thanks for joining me today. Thank you.