Dave Cole 0:00

Welcome back to security voices. I am here today I am Jacqueline, once again, a very, very busy retirement has claimed Jack's day, evening, week, month and so on. So all the best to him. In these wintry days wherever his path is taking him, I'm here with Allen Ohanian. Allen is the CISO, let me see if I can get this right of the LA Department of Child and Family Safety. That is correct. Yes. Awesome. And Alan just got back from Bahrain, where he gave a talk at a I'll let you do the name of the conference. Lest I butcher it. We did a talk on cyber psychology. So take us through it. First off, tell us why Bahrain, there's so many places you could do this. Besides everywhere. How did you end up all the way over in that part of the world?

Unknown Speaker 0:53

Well, thank you have a good morning. Good afternoon. Good evening, wherever part of the world that you are listening to this podcast a pleasure to be here. So bad rain. The food was great. Just kidding. That was not the reason of course not uprising. Amazing. Yeah. I had lamb biryani and it was so fresh tasted so good. Probably less hormones, or probably non and this left a taste on my mouth. So if I go back, I will definitely go for the food.

Unknown Speaker 1:21

Awesome. How did you end up there when you invited or yes,

Unknown Speaker 1:25

a few months back, I was invited to speak on an international you a cybersecurity conference in Summit back in Geneva. So the folks who were there, they realize this is an interesting topic. And many security professionals or athletes do what I see it's not focused on human element in depth. So this was a good addition to this barren conference, which was the first and one of the con in that region. It was Arab international cybersecurity Summit. Everybody from those region, including some folks from Europe also were part of that summit, the prints off background, he sponsored the event, mainly. So they started looking into cybersecurity as a huge initiative for the nation. And they're taking all the steps to collaborate, use innovation and the buzzword that goes around these days digital transformation, they want to kind of catch up with what the whole nation is doing. So it was a fascinating event. And it was truly a pleasure to be there. What was your topic? Cyber psychology? Yeah, take us through. Sure. So I decided to do something different. tackle it from a different angle. And the topic was cyber psychology and its impact on cybercrime. So we do all talk about human element. But rarely we go into the psychology of cyber world and internet and technologies that we use. Cyber psychology is basically where the technology and human collide. That's the shortest way to explain what it is. So historically, human beings have been social individuals who are used to have interaction face to face, resolving the COVID head, how that impacted everybody from going into offices back into their confined space of their own private homes, that changed people's behavior. So research has shown that the way we interact with technology and the way technology interacts with us, changes our behavior changes our psychology, when it comes to interaction, and when it comes to behavior in general. So my take was understanding how these changes impact user behavior, and how we can do a better job in not only preventing cyber crime from happening, but also becoming more proactive in designing technology and tools that is consistent with our new way of life, new psychology fewer, if you will, or new behavior. So that was the whole perspective to bring a different angle into this and shed a light so that we organizations can do a better job on understanding organizational culture combined with human behavior, and the technologist so they can design better tools that serves our current need. And it's consistent with human behavior.

Unknown Speaker 4:14

All right, so oftentimes, in presentations, you have an example of do this not that right? This is where it goes wrong. Did you have one of those in there? Give us give us an example.

Unknown Speaker 4:24

There are lots of examples of such and we do talk about for example, the fishing, right? This is very well known attack methodology that cyber criminals use because it's easy. It's very low cost and it's very, very effective. So we oftentimes prepare security awareness trainings, we go off the shelves by product, and we check mark yes, we do have annual security training, but less often we come back and realize okay, yes, people took these trainings, but how effective are these trainings? How much of that is consistent with organizational culture, the business goals the mission and from The end user perspective, what does it inform me? Why do I have to learn all these things, which is sometimes not directly relevant to the job that they do. So in our organization, LA County Department of Children Family Services, we do run phishing simulations, almost every month, we do a few of them. And what we do is we bring people back who are, quote, unquote, repeated offenders to see what caused them to click on certain links or certain emails. At first, it was interesting, because everybody was panicking Oh, my God. I'm calling into principal's office, what I'm going to say how I'm going to defend myself, but soon they realized that juncture is more of a collaboration is for us to learn from them and for them to learn from us. So it became teamwork. And then we realized people are just stating what caused them to let's say, click on certain links or take a certain action. And we learned a significant amount of knowledge from user behavior, because now we can redirect or have a different training modules available for them. So in case if they're come close to a like, attacks, they can better prepared and better protect themselves.

Unknown Speaker 6:07

That's an interesting one. So what did you learn when you asked them? Give us a fun story? Give us some of the insights that you took away from it? Sure. So

Unknown Speaker 6:16

he saw a range of things. For example, one user said, Well, I have an iPhone, how do I check to see if a hyperlink is malicious? And my iPhone is like, well, this is an interesting one. We never thought about that. So as security professionals, we know how to check that out. But from a user perspective, they weren't sure how they can manage that. Some of them are pretty basic. For example, they were unsure if that email that shows up that comes from the director or an executive individual, how should they respond? How should they check to see if this email address is the proper person sending email or it's a phishing email address?

Unknown Speaker 6:48

So pretty basic stuff, just stuff that standard security professional, what we'd hoped would be a standard cautious security professional would do intrinsically your DCFS. I think a lot of this stuff will probably make more sense if we had a bit more context on the organization. So before we get too far down into this, give us a primer on who that LA DCFS is and I'm assuming that there's a DCFS in every major city and so on. So to a certain degree like this could be extracted to a New York to an Austin to Seattle and so on, right?

Unknown Speaker 7:21

Yes, that is correct. Every each state that have Department of Children Family Services, they may be named slightly different. But essentially, the job of Department of Children Family Services is to protect children's well being and safety. So then about about ourselves. LA County is one of the largest nation in the county and so is its own single department. We have about 34 to 35 different unique departments within the umbrella of LA County, from sheriff's district attorney's office Board of Supervisors, county council probation, DCFS being one of them. So we are also the largest child welfare agency, the nation, we serve the entire LA County, which has a population of 134 5000 individuals employed by LA County is serving entirely County, we have about a $3 billion budget. Our budget comes from different sources state, local and fed, we do have a child protection hotline, which is very similar to 911 call. So when your crime happens, you call 911 for help, and we have something exact similar for reporting child abuse, we do receive about 230,000 calls a year, you can imagine how massive this number is. Each call creates a case that requires our social workers to go and investigate the nature of the call. We have about 81,000 referrals and about 128,000 children are custody. So the complexity of managing and serving the population as you can imagine, it's huge, just magnificent. I don't know how our social workers are doing it, but more power to them. They're doing an amazing job, how many of them are there, we have about 10,000 Plus individuals and employees, which vast majority of them are social workers going out into field day and night working tirelessly to make sure our children that are in our custody are protected.

Unknown Speaker 9:24

So it's your job not just to protect the infrastructure of DCFS, which includes ways of contacting you, which includes incredibly sensitive health data, incredibly sensitive topics. And it also includes protecting the social workers as well, which I think there's a lot of organizations that have sensitive data and even health data and potentially criminal data and so forth. But this angle of having social workers out in the field, in all sorts of settings is an extra wrinkle that most people working in cybersecurity, I'd imagine never have to deal with one of the unique angles of that, like take us through what it takes you to protect a social worker, how you threat model things for them, and so on.

Unknown Speaker 10:09

That is absolutely correct. So as I said about maybe five 6000 of our workers consist of social workers. And we have about eight different regions throughout LA County with 20 regional offices. So you can imagine how big of a population we do serve. As an information security officer. Clearly, our job is to protect the integrity, availability, privacy and confidentiality of data and information. But that's just a very, I guess, Canada terminology. When you start digging deeper, you realize how much complexity is in each element. And I just described from people process to technology. So we do get information from almost all over the place, mail, email, text, phone calls, referrals, all sorts, and then our social workers, when you receive this, it gets triggered to our different agencies that we work on law enforcement, probation, health services, psychological services, mental health, all these different elements then come together to combine and perform an assessment. Now, not only were obligated to make sure all this data and information that kind of collaborated across different agencies are protected, but the self individuals who are performing the job are also protected. Most of the time, when social worker walks into a house, when there's a case of referral, they have no idea what they're walking in themselves into, that can be very warming, nourishing family or else. So protecting their physical well being including protecting their information is absolute critical. So we have to face the public that we serve, but also take care of ourselves as well. That imagine

Unknown Speaker 11:51

protecting the information. I have a bunch of questions on that. But how much of your job involves physical safety of the social worker, I can imagine police wear body cams, probably a little extreme for a social worker, not the right message to send. But how much of your job is thinking through and making accommodations for the safety of the social workers out there? Is that somebody else's job? Or does that bleed over into you as well, your responsibilities?

Unknown Speaker 12:19

Great question. So they kind of blend in together. Part of protection of data and information has a direct consequence on the physical world. So the element of cyber psychology when we talk about in human behavior changes, there's a very symbiotic relationship between the physical world and the virtual world that we're dealing with. So what we do in the cyberspace impacts the physical world and vice versa. Now, when it comes to social workers, body cams, we don't use body cams, but it's not far to fetch because as I stated, the risk that a social worker can face physically, when they walk into an assessment home is high. Therefore, we do collaborate with internal folks and law enforcement to make sure their safety and well being is also preserved. For example, there was a time we were exploring to have an SOS type of button. So when in case they sense a life threatening incident or life threatening situation, they can always alarm, certain law enforcement agencies as well. We have also combined our efforts with law enforcement. So when there's a referral, usually law enforcement accompanies or social workers at a place that they're heading for obvious reason that as

Unknown Speaker 13:32

I just stated, so it's less of things you need to do in order to protect individual and more information flow and making sure when you get a referral, and you guys get it you the right people are there if it's a dangerous situation, police officer accompanies and so on. That is correct. So with respect to data sharing and information sharing across the different agencies that you said there, how messy is it, Alan? Is there a single system that you log into? Are you using like conventional SaaS applications? Like everybody's dropping it into box.com? and off you go, what does it look like when you have data that's coming in? Or a referral or an assessment? Do you remember that old I'm just a bill give us the Schoolhouse Rock version of it? What's it look like, man?

Unknown Speaker 14:18

Yeah, I wish it was that simple. I wish there was just one system and life would be great. I have a PowerPoint in my slides. When I show there's different positions, the CEO, CEO Oh, and then the CIO and assists Oh, it also shows how they sleep at night. Cisco is never in a bad sort of bed is empty. That talks about the volume and complexity of our world, especially these days. Well, social work is no different than any other organizational work that people do that deals with data and information. So the complexity, I'll try to dive into a little bit because it's very, very complex. As I said, we receive information from all sorts of resources. We have a state system, which is a closed system, and we get certain referrals through that and that's shared across State of California, we get referrals, as I said, from various means. And then this information gets dispersed into different agencies of health, mental health, probation, a law enforcement, county council and external entities that we do contract with. We work with a lot of nonprofit organizations, they do house, our children that are in our custody, and be contract. And some of those contracts, they have sub contracts that follows down to chain. That's just one piece from children perspective. And then we have our systems. So with COVID, the digital transformation for every organization, including ourselves accelerated, we started using Cloud more often, we started moving our data and information into different cloud systems that our social workers can easily access from anywhere on the world. I'll tell you a project that we recently did, and it hit the news, which was a using Amazon call center, modeling that and leveraging the technology that they have for our LA County DCFS call center, which allows us within 15 minutes, set up a call center anywhere on the world, as long as you have internet connectivity. So that by itself is huge. Yes, the efficiency got significantly high, we became much more robust on things that we do. However, that also created a whole bunch of security concerns for us, because now using the computing device, for a social worker, an individual who accesses these calls, protecting these calls, making sure only authorized individuals can see or access the transcript of this call is became a huge task, which we have to work with Amazon internally and externally with different folks to make sure we have enough safeguards to protect that information. Because if a call leaks out, or a parent who is angry because DCFS got hold up their children and place them in a better place to preserve their well being that can be a significant consequences for our social recruitment department, they can find out where the social worker leaves, they can find out where this child lives. And they can just go out there and make lot of soda say damages if they want to. So it's very, very high risk area that we have to be very, very cautious when we're working with different elements. So it's a very complex environment, if people are familiar with a database structure is more like a many to many relationship. So Cloud, different entities, organizations, and nonprofit public private sectors, and countless amount of systems that we deal with and work with. Because as I said, I wish there was one system that everybody will just go in there and find what they want. And not only that we have other entities such as nurses and doctors and medical practitioners, which feed into this data elements. So it keeps adding and becomes bigger and bigger over time.

Unknown Speaker 17:56

It sounds messy. It sounds super messy. Going back to it, how digital or social workers now on average, are they taking notes and recording transcripts? And that sort of thing right after a meeting and putting into a system has all of that been digitized? So it can be combined with things like electronic health records, and that sort of thing? And now, if they have how recent is that? Is that a recent kind of COVID related change or just part of standard digital transformation? How kind of far ahead or far behind? Are you?

Unknown Speaker 18:27

Yeah, excellent question. So historically, government agencies are far behind a private, the digitization process is far slower than private sectors. Certain initiatives, including like Amazon, call center a we did start this while back, but COVID Fortunately, it helped us to accelerate this transition. When it comes to different systems and different elements that we work to make sure this data stream or collaboration is in place. COVID just made it become faster, we kind of started transitioning into the cloud far faster than we thought we would do in a transitional or in a non COVID situation, because now everybody's obligated to work from home. And not only that, we have to make sure the systems are available to the social workers to do their jobs. Digital transformation, we have boxes and boxes box of paper copy. So as you can imagine, because when a call comes in, not every system was in a digital format or an electronic format so our social workers could enter information there are certain pieces but not all. So we are moving towards digitizing all of our paper documents, which is a significant financial and human resources, perspective elements, which we can take all this paper copies of fears and years of case files making a digitized. So of course it helps us from a various perspective. Now we can digitally share this information over let's say our health providers or healthcare providers. We can share this with our law enforcement people, our county counsel who was advising us on different cases. So that's one of our major initiatives that's happening as we speak. As far as technical IQ or TQ, we can call that tq. We had, of course, a learning curve for our workforce members to make sure they all have the proper technological training to use those different tools in the county. The LA County DCFS is the largest department with departmental issued iPhones. So we went with the platform, my phone for obvious reasons, closed ecosystem, the bridge on iPhones are far harder than Android phones. So we decided that iPhones probably were better suited for our users from security, privacy and usability. So we have the largest. Absolutely yes, all of them do have an iPhone, and we have an app store for us. So we can approve what applications can be stored, when can they use and what cannot they use. So it's all gets pushed out from our mobile management system, into the social workers county issued mobile devices. So there is a trusted area, if you will, that social workers can use different technology and tools and apps to do their jobs better and much more efficient. Historically, there was a time where social workers would go out, do their assessment, write their notes, and then come back and rewrite them into a system. But now we are leveraging a system where if the internet connectivity is not there, it stores the information when they're back to the offices or when they're back to a place where they have internet connectivity. It syncs up to the cloud.

Unknown Speaker 21:36

That sounds super reasonable and saves a lot of transcription later if they just start by dictating and voice dictation, provided that you don't have any international names. In my experience, it works reasonably well. So that's pretty cool. So what do you worry about? Is it mostly protecting all of that data? I mean, you have enormous amounts of sensitive data. And I'm assuming at this point, it's going up into the public cloud, either into SAS services or into Amazon or somewhere else. What do you obsess over since you're not sleeping? What's keeping you out of bed and up at night? Yeah, I

Unknown Speaker 22:11

wish it was one thing. So as you already realize it's code encode a complex environment data comes in and out of every other angle that you can imagine any county, we have a department called internal services department. So they do redirect traffic. And they do have their own data center. So that's pertaining to LA County. But in the meantime, we do have government cloud services, which we work with a few giant companies, Google's and Microsoft, and Amazon, and so forth. So we do also share data on those platforms. And then we have to make sure these platforms talk to each other because sometimes one system is hosted on, let's say, Google, but some systems are hosted in Microsoft. So we have to make sure that connectivity is there. And clearly, security of those elements become a critical job for me and my team. What keeps me awake at night is I used to joke with my boss, ex boss, he retired all about that. It feels like we are in a universe where asteroids can fall out of the sky at any time. So always be ready for unexpected events that come down. System on availability is one of our huge athletes. For me these concerns, yes, the protection and unauthorized access to systems are very, very important. But if a social worker is out there, and they don't have access to their systems, or vice versa, if somebody wants to inform of a critical situation that a child is, and they can't get hold of us, that can be fatal. So that connectivity and availability. So to say uptime is absolute critical, and that can be jeopardized, from various perspective, technical or non technical, manmade or accidental. So let's say if you have a DDoS attack, or if we have a malware that brings the entire system down, cripples all the files, that becomes a huge deal for our social workers in our department.

Unknown Speaker 24:08

So we think back to the classical CIA triad, it's availability, availability, availability, for all sorts of obvious reasons. Actually, it sounds like health care providers, critical infrastructure. I mean, you guys kind of exist at the nexus of that the combination of those so it makes perfect sense that it's availability, how much is cloud helped? And how much does cloud hurt? I'm listening to this. And it sounds like great, it things more available in the cloud. Of course, you can stand up more services and be more responsive. And certainly for availability, there's a ton of advantages being in the cloud. But what's the complexity trade off? And what's the downside, so give us the pros and cons because it was one of the reasons why I wanted to talk to you. And when I grabbed you in the hallway at the conferences, because you were talking about cloud and government, and first of all if you're in my hometown, so of course when I gotta wanna hear more from Alan and meet the guy. But also is interesting because of all things they didn't expect would be someone speaking in forward leaning ways tech for ways on Cloud inside a local the Los Angeles County. So that was really cool. What's the pros and cons give us some of the history of cloud and LA County and DCFS?

Unknown Speaker 25:21

Yeah, absolutely. Dave, great point. And I think it's a great topic, especially these days. So I remember when the cloud first started booming, and cloud providers started promoting the product. I personally am on with other professionals and co workers who were not for it. Because the platform was still raw, not many visibility or governance were shaped around the cloud environment. It sounded nice, it sounded great. But in the meantime, we held off because we didn't see the platform is mature enough to move our data and started leveraging or utilizing cloud. As time passed, cloud providers became far more advanced, they started building much more measures that can help organizations to better protect what they're putting out there. I use this example as you can have a Ferrari, which is a great car, car guy, by the way. But if you don't have the proper driver, or you don't have a train driver to drive such a car and go in a race or drive a Formula One car, it's absolutely useless. So with that transition into cloud, cloud providers became far better in that what they do, which means they provided much more granularity, much more security controls and measures for organizations to leverage. But in the meantime, the challenge became, do we have enough trained people to use Cloud for exact same example that I stated, do our team? Do our workforce members know how to leverage cloud environment? Do they know how certain security and privacy controls should be configured should be turned on? So it was a huge learning shift from hands on prem? Versus now I have to learn and relearn maybe certain things that I used to know how the cloud operates. So that's one aspect. And then oftentimes, I'm asked whether it's a good move or not. So it's not that easy to answer. There are various elements to consider each organization and business is different. So in my opinion, that assessment comes down to how much of this makes sense for me to move my data into Cloud, financially, human resource perspective, availability and confidentiality purposes. Sometimes for organizations, it's much more prudent if they use on prem, that makes sense for them from business perspective. And sometimes, like us, we do a hybrid model, some data is on prem, some data moves to the cloud. So it ultimately comes to the organizational maturity and business understanding of what am I trying to get out of kludges cloud? If we speak 20,000 feet makes sense, far less cost, far less maintenance costs. But then we start digging deeper about different branches within the cloud. How much of this is making sense for my organization? Is this relevant to me at this point, or my workforce is not even ready to start using cloud? Do I have enough human resources that they can manage cloud environment? Do they even understand what the cloud environment looks like? And then regulated data? How much of this data I can place in a cloud? Having much more confident that it's much secured and on prem?

Unknown Speaker 28:33

And you don't have to give me super specifics on this. But just give us a sense how much of what la DCFS is doing as on prem versus St. Cloud? Where are you guys in the transition? Is it 5050? Is it 3070?

Unknown Speaker 28:47

Putting percentage on it. So let me think so I would probably say somewhere between 40 to 60% range, we have our systems and data on prem. Gradually, we're transitioning them into the cloud environments. As I said, as our model matures, as our data becomes much more secured in fashion that we can move and kind of forklift everything from on prem and moving to the cloud. I'll give an example. We have a closed systems statewide provided system which obviously that has to stay on prem. from the technical perspective and sensitivity of data. We are still working progress. There's few miles away offshore until we move these things to the cloud. But for public information and systems that are less critical, it's easier to move. It's easier to transition and certain elements, as I said, which are, let's say legacy systems legacy applications, they still reside on prem. And that includes the data to part of this whole transition and working with different data elements includes communication between cloud and on prem. So we have certain data elements on prem and certain In things on different cloud providers, so we do want to, at the end of the day want to have a solid data about, let's say a case, right? So we have to grab from different parts of the world, bring it together and make it one unique and united data stream. So that transition is still happening. And as I said, there are a lot of elements to consider, from your human resource perspective to your budget to the complexity of environment and how much visibility you can have, and how much data can be offloaded into a cloud environment. So it's not as easy as some people imagine.

Transcribed by https://otter.ai