uberknowledge

Lester Godsey, CISO for the City of Mesa, Arizona

The Ever-Changing Role of a CISO

Lester presents his measured thoughts on the critical skill set for the future CISO and the challenges they face as the role evolves. He offers a frank opinion on the need for vendors to cooperate and present solutions to the market that will play nicely with others.

Ashwin Krishnan: [00:00:01] Welcome everybody, with me today on the podcast I have Lester Godsey, who is the CISO of the City of Mesa, Arizona. Lester, do you want to introduce yourself before we dive in?

Lester Godsey: [00:00:14] Yes, Lester Godsey, like Ashwin said, I'm CISO for the City of Mesa. I've been in the IT field for around 24 years. The vast majority of my experience has been public sector, so higher education and local government. I also teach part-time for a variety of different universities. I do a fair amount of presentations and writing in my spare time as well.

Ashwin Krishnan: [00:00:42] Excellent, there's a good dovetail into the writing aspect. I'm actually reading the headline from a really interesting article you wrote for CIO magazine and it's called, "Cybersecurity Considerations in Selecting an Enterprise Backup Solution." So, first off, the title blew me off, I have to be honest with you. Enterprise backup security, come on, what's going on here? As I started reading the article it became pretty apparent that there is a big security component to enterprise backup and we definitely want to touch a little bit on that. But for a minute let me take a broader perspective. What you have alluded to in this article is something that is at the intersection of a CISO's mandate and a CIO's mandate.

[00:01:27] Do you think conversations like this, on security and backup, are starting to happen within enterprises? Where CIOs are starting to realize, "Hey, the second or third tier backup that's happening over there, if we don't have the right sets of security controls like key management, etc., we are opening ourselves up for attacks." Can you talk a little bit about that?

Lester Godsey: [00:01:49] Sure, it's my hope that that conversation has already begun between CISOs and CIOs. That's making the presumption that in most organizations, and I haven't done the research, but I'm going to go out on a limb and say that CISOs generally still report to CIOs. From a CISO perspective, at least my interpretation of my role and responsibility, is to take the whole IT organization and the enterprise services that we provide collectively. Look through all those and then identify where the risk is associated with service delivery. So, not to get on a soapbox, but one of the first things I think a CISO should do, and continue to do constantly, is measure the risk within the organization. Identify and create a risk management plan and then as things come up you can identify what those risks are. Communicate with management and have a discussion about whether that level of risk that's been identified is acceptable or what can the CISO do to reduce that risk down to a level that's acceptable to the organization.

[00:03:00] So going back to the article, the intention was to point out something that on the surface would seem pretty innocuous. Every organization has a strategy and a service they deliver with regard to backups, but maybe not every organization thinks about that service in the context of security and what the risks are.

Ashwin Krishnan: [00:03:20] Correct, and to extend that argument further, does this also mean that increasingly, for example when you have backup and restore vendors come and chat with the IT organization, the CISO or their team members need to be part of the conversation? You need to impress upon the vendors that it's no longer kosher to just talk about speed of backup, availability, and restore capabilities, but also about what they are doing to ensure the backups are secure and encrypted, etc. So, there's a bigger goal here, right, where you want to actually influence the vendor road map?

Lester Godsey: [00:03:56] Oh absolutely. Security should be integral in any sort of road map discussion, regardless whether it's infrastructure backup, application data, analytics, you name it. Conversely, from my perspective, I try to extend the same courtesy. I give my management regular updates as to the cybersecurity program here in the City of Mesa. I solicit feedback from them and do a temperature check on what that risk is, and amongst the management is also our enterprise architect, for example, so it's a two-way street. Security needs to be involved in all those discussions about application and infrastructure road mapping. We – or in this case me - need to communicate what the risks are and what the proposed direction is to those responsible for the road mapping.

Ashwin Krishnan: [00:04:48] Okay, so that leads me to a follow-on question. In terms of the changing face of a CISO's job description in an enterprise today versus years ago, what is it going forward? If you were to chart what an ideal CISO's skills look like today versus 10 years ago, where do you think some of the changes have happened? Do you think there's going to be a new breed of CISOs who are forced or required to think differently to be able to connect with these various stakeholders and continually provide updates in a language that those stakeholders can understand?

Lester Godsey: [00:05:31] Absolutely. The funny part is your timing is excellent in that I spoke on a panel this past Friday here in Phoenix at The Phoenix Physical and Cyber Forum. One of the questions that we were discussing was the role of physical security and is that something that should be under the purview of a CISO or CSO. The nature of the conversation was along the lines of, "It's hard enough to find a unicorn. It's getting down to the point where you're now looking for an animal with two horns, you know?"

[00:06:12] So, to your question, there's so many things that would be ideal to have in the perfect CISO. You have the physical security, some organizations may want elect to have that under one body, but what's the likelihood of somebody having those cybersecurity skills as well as really well-defined and mature physical security skills? The physical side, so not to diminish that, the trend I see is a continued enhancement on the CISO's ability to speak the business language. About 10 years ago a CISO's vocabulary might have been, this is a gross exaggeration, but it might have been limited to "No" and "No, you can't do that." Versus CISOs today who should be cognizant of what the business's vision and mission is and have the mind frame of, "How can we enhance our organization's ability to make good on that mission and vision but do so in a way that's secure?"

[00:07:30] I think ongoing knowledge of what the business schools are, what they are trying to accomplish, and how we can affect it in such a way that is secure is critical. Then the biggest thing is, and you may have seen this ongoing theme in some of my articles, I envision that the future CISO is going to have to be really capable when it comes to data analytics. The industry is very focused on tools right now, so your SIEMs, AI, machine learning, all those buzzwords, but at the same time at the end of the day it's all data. The lowest common denominator, whether you're talking about cybersecurity, whether you're talking about traditional IT organizations, all organizations are becoming more and more focused on making better data-driven decisions. Having a good understanding of data analytics, I think it's going to be a critical skill set for a future CISO.

Ashwin Krishnan: [00:08:34] That's a great prognostication of where things are going. Let's go to a set of questions that I've used in other CISO conversations as well; just to get to a broader perspective on the issues. The first one is, in your opinion what's the most understated but really critical security issue?

Lester Godsey: [00:09:00] Honestly, the first thing that comes to mind is the basics. I'll just use local government as an example. I'm not saying this makes it specific but a lot of municipalities, a lot of government agencies are very fixated on smart cities and certain hot initiatives. From a cybersecurity perspective, what are we trying to do to help facilitate that conversation? But at the same time, you still have to do those things like vulnerability remediation, scans, and constant back and forth on putting mitigating controls in place to minimize risk. So, there was an article that came out not too long ago about T-Mobile losing millions of records. It showed this happens to large organizations, it's not just government, but a lot of this, just the basics of eating your vegetables, from a cyber security perspective, for whatever reason, just seems to still be very undervalued within any organization.

Ashwin Krishnan: [00:10:11] Yeah, it's almost surreal you mention this because this is one of the few questions that drew the same rhetoric from all of the CISOs: just do the basics.

[00:10:26] So, just kind of double clicking on that, you mentioned smart cities and IOT, etc. This is what the boards, actually this is what the competitors and other government agencies are looking to get budget from. Now does the CISO need to have cognitive dissonance? Where on the one hand they need to be able to go and talk about these smart city initiatives to secure budget and mindshare, while not getting caught up in his or her own rhetoric but also be able to go back and, like you said, make sure that the patches are installed, the CVEs are addressed and so forth? Is that something that you think is one of the top challenges for CISOs?

Lester Godsey: [00:11:11] Oh yeah, absolutely. It's almost like you need to have a toggle switch, so you can flip when you need to, right? On one hand, I'm having executive level discussions about how our City of Mesa IoT strategy, which I'm responsible for, aligns with what the needs are for our Smart Cities Initiative. Having conversations with multiple departments within the organization and having regional-level conversations along those lines. Then flip the switch, and I go back to reality, getting our arms around what not only the physical architecture associated with our IoT environment looks like, but also what the data architecture looks like. How do we put security controls in place to ensure that we've mitigated the risk down to a level that's acceptable to the organization? And then having the conversation in between, with regards to what's the risk associated with IoT and separating hype from reality.

Ashwin Krishnan: [00:12:20] Very interesting. It's definitely not an easy job. My next question is, what's the most overhyped security issue?

Lester Godsey: [00:12:35] Overhyped security issue...

Ashwin Krishnan: [00:12:39] Blockchain?

Lester Godsey: [00:12:41] Yeah, that actually was coming to mind. I was trying to come up with something maybe slightly different, but yeah from my perspective, blockchain is hugely overhyped. I think the technology is still very immature and from a business use case perspective, especially in my area, it's nowhere close to prime time. From a maturity perspective, I've done some research as you might expect, just the sheer amount of compute and resources required to effect a blockchain solution within any significant size organization is significant.

[00:13:26] I think until we can overcome that, that's just one technical hurdle. I work for a city and I don't think from a business use case perspective it makes a lot of sense to invest resources into blockchain technology that's going to be restricted just within the City of Mesa. Now if we were to do something at the state level or even better comprehensive federal level then it might make sense. Especially at the state level there's a lot of services, and a lot of communication in the way we deliver services that are dependent upon state services. If we have that wider community, then it would seem to make sense that other municipalities would then join into a single blockchain implementation, if you will, with that shared ledger all that other stuff. So in that sense, scope and scale, it has a direct impact of usability in my opinion.

Ashwin Krishnan: [00:14:29] What in your opinion is most broken when it comes to security today?

Lester Godsey: [00:14:39] I'd say one of the things that is most broken is how we have to put together all the tools, all the services to gain insight into what the environment looks like, what the risk to said environment looks like. And ... I hate using this phrase, because I can't begin to tell you, I'm shocked whenever a vendor actually talks to me and doesn't use the phrase, "single pane of glass." I just want to hit myself with a two by four every time I hear that that phrase. But I guess in this context it works. There are so many threats, there are so many risks, and I'm not advocating that there should be a vendor that comes in and tries to do everything and be everything to everyone. I just don't think that's feasible.

[00:15:43] At the same time, and Ashwin you have a better insight than me, part of me wonders pessimistically if vendors are just inherently not good at working together with their competition. This concept of standards, and I'm not talking about the common frameworks or anything of that sort, that's pretty straight cut and dry, but when you have these different, disparate systems and our job as security professionals is to get our arms around the risk and the threats of our environments, but we have 10, 15, 20 different tools. You see vendors not having good APIs or web services that are securely developed or even available to the solutions that you bring in-house. There's no data dictionary or ERD that, even if you wanted to do something custom and integrate multiple disparate systems together, you don't even know what you're looking at with data, it just runs the gamut. That's been one of the frustrating things for me. If all the security vendors are out there trying to make my life and my environment better, they have to understand that all these pieces have to work together.

Ashwin Krishnan: [00:17:10] That's a great one, you're right. Having come from the vendor space myself, I think the compulsion, or the lack of it, to work with the competition and make it easier for customers is not something that is top of mind.

Lester Godsey: [00:17:26] And not to be too facetious, and not specific to security vendors but IT vendors in general, in the 24 years I've been in this business I can count literally on one hand the number of vendors who actually had accurate and mature data dictionaries or ERDs that document what their back-end data structure is. And why is that important? It is important because more and more I'm looking for integration skill sets. I want to be able to take disparate data applications and get them tied together to give myself that supposed single pane of glass and vendors are horrible like that.

Ashwin Krishnan: [00:18:12] Moving on, where have you and your fellow CISOs that you've spoken with spent a lot of dollars but have seen little to no ROI?

Lester Godsey: [00:18:28] So two things come to mind and for different reasons. One of them is actually the SIEM area. I think that's a mixed bag, and maybe this is the way it's pitched, but I would also argue that my fellow CISOs or security professionals should be smart enough to kind of be able to distinguish between vendor-speak and reality. They get the SIEMs implemented and then they think it's going to solve all their problems. They just don't work that way. It's not a vendor issue, it's more along the lines of, "Oh, you mean I have to do alerting, you mean I have to constantly update my queries and my dashboards for new threats?" I mean, it's not a small investment, right? And then depending on the SIEM and what model they use from a licensing perspective, some of these companies will just digest tons of data while they put themselves in a position where they can't afford it anymore. I'm not saying there's not some vendors out there who will remain nameless who aren't charging a lot of money, but SIEMs are one of the areas.

Lester Godsey: [00:19:54] The other area is professional services, consulting, that sort of thing. I recently went through one for our IT department. I think we paid a pretty hefty sum and what we got out of it, in terms of strategic planning and things of that sort, I kind of question what the value was, but I'll leave that one alone. So, those are the two that come to mind.

Ashwin Krishnan: [00:20:19] Okay, that's good. Any parting words for your fellow CISOs about how they need to work differently, act differently, and connect differently in this new world?

Lester Godsey: [00:20:37] Yeah, so I'm trying to avoid saying the same thing over about eating your vegetables. That aside, I have found, and again I've learned through my own mistakes as well, spending the extra effort and time to put the appropriate frameworks in place to ensure that your program becomes operationalized. What I mean by that is, for example, our earlier discussion about a risk management plan. I can't begin to tell you what a long and arduous process that was. I did it myself. I spent a lot of time outside my normal day doing it, because I'm too busy during business hours. But once I had that in place, everything else became easier: conversations about managing priorities based off of risk or enterprise efforts where I was asking for budget and things of that sort. Having that framework in place and a risk management plan that I referred to on a regular basis with management has been hugely successful. I'm convinced that if I didn't have that in place certain initiatives that I hadn't planned for, things that came up wouldn't have been funded for example. It's just stuff like that. All the framework and the strategic planning, going through actually creating something along those lines and then operationalizing it — it's a large investment of time upfront, but I think it's been well worth it.

Ashwin Krishnan: [00:22:18] Got it. Finally, for the vendors again, could you give three pieces of advice: start, stop, continue. Something they should start doing, something they should stop doing, and something they are doing right that they should continue at.

Lester Godsey: [00:22:39] Honestly, I'm hesitant saying this because I've got to think the statistics are such that it's somehow working for them, but at least from my perspective, stop the cold calls. It's funny, those e-mails would start off with, "Hey, can I have an hour of your time." Then it dropped down to 30 minutes. The last one I had was asking for three or four minutes. I'm thinking, "OK, whatever." But it's got to work some percentage of the time because they refuse to stop doing it. It doesn't work with me, I guess that's what I'm trying to say.

[00:23:29] So, things to start doing. I guess this is twofold. First, if you are going to try to reach out to me, demonstrate some knowledge that you made some effort to get to know what my organization is like and what my needs are. That definitely would be a plus. Second, understand what your limits are and what your product or services are good at and what they're not. Don't try to be something that you're not. I've had some really interesting conversations lately along the lines of, "I wouldn't expect you guys to do this, this, and this; it just doesn't seem to make sense." I would say, start being realistic about what it is that you bring to the table.

Ashwin Krishnan: [00:24:29] And then continue - anything that you think they're doing OK or well?

Lester Godsey: [00:24:35] I think some vendors are taking the approach of finding ways that makes sense to build contacts. I'm not talking about like the state dinners or the like. You just got back from Black Hat, so I'm assuming you drove a couple of Lamborghinis or whatever. I mean being part of organizations that focus on the C-levels and having meetings and discussions set up in such a way that they're designed to add value to both parties. I don't want to come across like all these vendors should cater to and do all the Lamborghini things for the C-level folks, but I am suggesting that there's a better way and there's a more efficient way where both parties can get derived value. Like, for example, Advanta, what they do along those lines seems to work pretty well, at least for me.

Ashwin Krishnan: [00:25:47] Got it. This has been really, really interesting and I hope the listeners get as much value out of it as I did. Thank you for your time. Let's hope to catch up with you on a future podcast.

Lester Godsey: [00:26:00] Yeah, that be great, Ashwin. I enjoyed it; thank you.

Main discussion topics:
1:49 The conversation that CISOs and CIOs need to have
3:20 Should CISOs be influencing the vendor road map?
6:12 The critical skill set for the future CISO? Speak business and know data analytics.
10:26 The challenge of the duality of the CISO role, aka: the toggle switch
12:41 Blockchain is today's most overhyped security issue
15:43 Vendors don't play nicely, but they should because CISOs are seeking integration.
20:37 Take the time to implement proper frameworks; they will streamline your processes.
23:29 Vendors should be realistic and honest about what they bring to the table.