uberknowledge

Lester Godsey, Chief Information Security and Privacy Officer, City of Mesa

Ransomware and Local Government

Lester talks ransomware in the government environment, cybersecurity insurance, and data privacy as a two-way street.

02:21 Government is known for being bad at cybersecurity and for purchasing cybersecurity insurance. This makes it a perfect malware target.

05:47 Don’t rely on cybersecurity insurance; it’s not a cure all. Look at your overall security framework instead.

13:23 Privacy is an issue with duality. Citizen’s data privacy must be respected, but to provide enhanced services, you often need access to personal data.

Ashwin Krishnan: [00:00:41] So welcome to what we are calling the Cyber360+, which is an evolution of the UberKnowledge podcast, where we have 10 or 11 of our past guests in an ongoing dialogue. So, I have the pleasure today of talking to Lester Godsey, CISO of the City of Mesa, Arizona. Lester, welcome and happy Friday to you.

Lester Godsey: [00:01:02] And to you as well, Ashwin.

Ashwin Krishnan: [00:01:05] Let's talk about a topic that I believe is at the top of your radar, and I believe that of your peers as well, not just in local government but in higher education, etc., and that is the topic of ransomware.

Lester Godsey: [00:01:21] Yeah, ransomware. Obviously, it's been around for a while, but it's interesting how it's had a resurgence in popularity or, to put it in security parlance, increased risk to the organization.

Ashwin Krishnan: [00:01:36] So, what has changed? Like you mentioned, this is not something new. We've talked about ransomware for a long time. Why is this getting so much attention as it relates to local, state, education institutions? People that otherwise you wouldn't think as a high value target.

Lester Godsey: [00:01:57] Yeah, for sure. I think there's a couple of variables. One thing I want to start off with is, at least from our data that we've seen in the City of Mesa, a couple of years ago, ransomware was really high from a threat profile perspective. Then we started seeing that kind of fall off, and we saw more in the way of cryptomining, malware, and things of that sort. And it's not until the last six months or so that ransomware has kind of reemerged again as a priority from a threat perspective.

[00:02:21] But to answer your question, I think there's a couple of variables along the lines. I think one is just, in particular, government, and this might be more unique to government than a higher ed, but just the profile of local government. A lot of research studies have shown that government, whether you agree or not, is one of the worst sectors out there when it comes to cybersecurity and our maturity along those lines. So that's a fancy way of saying maybe easy pickings, to be blunt.

[00:03:10] Another thing is local government, more and more, when I talk to my counterparts in Arizona and throughout the country, whether you're large or small, it seems like everybody is buying into the concept and has cybersecurity insurance. I haven't seen data along these lines, but I have to speculate that the threat actors now know that here's our target sector, and if nothing else, they have poor defenses and they have cybersecurity insurance, so, they may be more inclined to actually pay. So, I think to reassert the resurgence in the ransomware is, well, it's kind of a supply and demand. I think it's a situation where they know that this is an audience that has a propensity to pay.

> "I think it's a situation where they know that this is an audience that has a propensity to pay."

Ashwin Krishnan: [00:04:13] Wow, so that kind of makes it a no-win situation, right? I'm the bad guy, and I look at you as Lester and think about the City of Mesa, they obviously have bought cyber insurance. So, if I come to you and say, "Hey, this is my offer to you and it's below what your insurance company is willing to pay," then chances are you want to say yes and move on with life. So how do people like Lester and his counterparts come to terms with yes, we have cyber insurance, and yes, our ability to guard needs to get better, but mentally ... Well, walk me through how you would go about explaining cyber insurance is not a cure all. In fact, it's like you mentioned, it makes us a sitting duck, and therefore we need to bolster our defenses and get more proactive about this.

Lester Godsey: [00:05:06] Oh, yeah, absolutely. So, a couple of thoughts along those lines, at least from our perspective in the City of Mesa. We don't have cyber insurance for the sole purpose or even the purpose, I should say, of paying ransoms. We have cybersecurity insurance for those other ancillary needs that we have in case there is an incident that we have to address. So, you know, bringing in third parties to do forensic analysis, assist with investigations, clean up, etc. So, our mentality in the cyber insurance portion is along those lines and not paying.

[00:05:47] And so I think that's something that all organizations, but government organizations in particular, need to have the mind frame of because you and I have had plenty of conversations with many people, and the philosophical question is, do you pay the ransom or don't you? And there's pros and cons to that. Every organization needs to make that decision for themselves. I would say that you shouldn't count on cybersecurity insurance being a crutch because just like any other insurance policy, once you get hit, you know, the expectation is either your rates are going to go up, or you might wind up being uninsurable, etc. So, it's not a cure all. And if an organization, ultimately, is interested in getting into being realistic about root cause of vulnerabilities that exist from a cybersecurity perspective, the insurance is a nonstarter. You really have to look at your overall cybersecurity framework, if that makes sense.

> "You shouldn't count on cybersecurity insurance being a crutch."

Ashwin Krishnan: [00:06:51] So let me ask you, from a perspective of taking every bleak situation as an opportunity to get better, is this now giving you and your counterparts in other cities and local governments the ability to be on the city council agenda; the ability to actually ask for more budget; the ability to actually show ongoing risk reduction capability? Is there a positive aspect, if you will, to having ransomware be that stimulus to actually have a conversation on an ongoing basis? Because even if you're not getting attacked, your sister city is. Therefore, it's not like you don't have the opportunity to use that as a lever to continue having this dialogue, or are you seeing CISOs still being a little more circumspect about talking about this?

Lester Godsey: [00:07:53] The short answer is yes. If you're looking for some silver lining in this scenario, that is one of them. From my experience, I would qualify that by saying the silver lining has a relatively short shelf life. And what I mean by that is, it's just like anything else. I liken it to car alarms. When they first came out, they were very useful. Everybody paid attention to it. But I mean, these days you can't ... it's getting to the point where, even at the local government level, it's almost like every day — or it feels like that, I'm sure it's not the case — but every day you're hearing about this city or this government was successfully hit by ransomware, or this university, whatever the case is.

[00:08:41] So I kind of feel like my job is not to necessarily say that the sky is falling, but in an appropriate, realistic way, use those examples to help frame the story that I'm trying to communicate to, in my instance, elected officials, or for somebody in the private sector, to their board. But part of the concern is if we keep on having this same story told over and over, it's going to lose its effectiveness. And people are going to become kind of deaf or blind to the issue at hand because it's been so saturated.

Ashwin Krishnan: [00:09:22] So that's a great point. I think the fatigue sets in certainly. And then, too much information is something we all have to deal with constantly, correct?

Lester Godsey: [00:09:31] Yes.

Ashwin Krishnan: [00:09:31] So, asking a more technical question — and this comes back to what you were mentioning earlier about city, state, local governments probably not leading the pack when it comes to cybersecurity — in terms of the citizens' assets that you're protecting, whether it's local returns, whether it's property taxes, there is a ton of information that is hosted by the state local government, is there a better sense of our understanding of, do we know where our critical assets are? Are we keeping up with that?

[00:09:31] I'm just going back to awareness. Like you were saying, while ransomware may not be the cause for having this conversation every day, but understanding, we just expanded into this new neighborhood; we have 10,000 more residents joining our community; we need to keep up with where their critical data is stored; is there an appreciation for that also showing up as a result of this?

"Part of the concern is if we keep having this same story told over and over, it's going to lose its effectiveness."

Lester Godsey: [00:10:37] Oh, absolutely! Really that's one of the unique challenges, in my opinion, with respect to government as a sector, in that, our constituents might be the same folks as on the private side with consumers, but the nature of the services that we provide are fundamentally different. Oftentimes that is centered around data, specifically personal data. So what's been an interesting, I guess, confluence of events or initiatives on our part, at least with the city of Mesa, is just our day-to-day services, initiatives that we are strongly working in. So, we have a smart city initiative that's well underway, and one of the common threads is data privacy. Actually, just a couple of months ago, I also assumed, in addition to the CISO role that I've been in for a while, the chief privacy officer role because we recognize that as a city, we have residential business information that's of a sensitive nature and we have a responsibility to protect that. So whether it comes to malicious attempts like ransomware or data leakage, like somebody didn't configure an S3 bucket properly or anything and everything in between, we have that core responsibility, and what are we doing along those lines to ensure that data that is private, stays private?

Ashwin Krishnan: [00:12:12] Got it. That's the first I've heard of a chief privacy officer in a local or state government, but that's great.

[00:12:22] Now, you mentioned private sector and consumer. Putting your hat on as chief privacy officer for the citizens of the City of Mesa, is there an expectation of awareness when it comes to your constituents? Again, using the analogy of the private sector and the consumer and that basic understanding about not having location turned on all the time, etc., but given the wide demographics I assume in your city and other cities, is there more of a one-sided responsibility that you and your team share? Or do you still believe that there is awareness and there is, I mean, activism is probably too strong a word, but at least an understanding of the nature of, let's say, an app or even filing your local property taxes that you believe the citizens need to share as well?

Lester Godsey [00:13:23] So, that's a great question, Ashwin. My answer is, it's not necessarily just one-sided. And so, the stance that the City of Mesa has taken is — and this is an ongoing effort, just to be clear — we do have a series of what we call data privacy principles that are posted on our public website under our Smart Cities initiative, and the principles actually address that. It's not a clear delineation of black or white when it comes to privacy of data because the very nature of the services that we provide, and we want to continue to enhance, oftentimes require access to citizen and resident data. So, when we're talking about enhanced abilities, it's to not only do utility payments but one of the things we're actively working on as a city is enhanced automated meter interfaces (AMI). So, being able to do things down the road like automated turn-on and turn-off of services to enhance the user experience, but a prerequisite of that is having access to personal data so we can do that.

> "It's not a clear delineation of black or white when it comes to privacy of data."

[00:14:39] So, our privacy principles are centered around and acknowledge the fact that, in order for us to provide enhanced services, we need access to this data. But when we're in a position, we will let you know how we're leveraging that data for services. It's interesting you used the word activism. I think what we are striving for in the City of Mesa is more of a collaboration, and an education and understanding on both parts: what's important to our citizens and also educating our citizens that we're not collecting data just for the sake of collecting data. We use this data in order to provide you X, Y, or Z service, if that makes sense. So, it's really a two-way relationship when it comes to data.

Ashwin Krishnan: [00:15:26] Now, that's a great insight because lots of times you forget that there are utilities, like you said, the AMI initiative, which is really allowing for better monitoring and energy usage and overall reducing carbon emissions. So that's great. I promised myself I wouldn't use the phrase smart cities in this conversation because we've going to save that for a later date.

Lester Godsey: [00:15:49] OK. Fair enough.

Ashwin Krishnan: [00:15:50] I'm not going to ask you any question on smart cities; I think that's obviously a very, very important topic.

[00:15:56] So this has been great. Lester, I appreciate your time and you joining us. In the future, we're going to talk about smart cities and other smart initiatives besides, digging a little deeper into topics like we did today on ransomware. So, again, I appreciate your time and have a great day, Lester.

[00:16:16] You too, Ashwin. Thank you.