

Data Security within State Government – an Interview with Mark Weatherford CISO for the State of California

Listen to Podcast [here](#).

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.

Joining us today is Mark Weatherford, Executive Officer California Office of Information Security and Privacy Protection. Mark Weatherford has extensive executive and operational experience in the information cyber-security arena. With a career that spans both public and private information security sectors.

Appointed by Governor Schwarzenegger to his present position as Executive Officer of the California Office of Information Security and Privacy, Weatherford has a broad authority over the state's information security and privacy activities.

In his role, he is responsible for California State Government information security and privacy program policy, standards, procedures and also for coordinating the activities of state agency information security officers to ensure compliance.

He also oversees the first in the nation Office of Privacy Protection, which provides information education for consumers on identity theft and other privacy issues as well as privacy practice recommendations for business and other organizations.

Mr. Weatherford previously served as the Chief Information Security Officer for the State of Colorado where he was appointed by two consecutive Governors to develop and lead the Information Security program. Mr. Weatherford is a formal U.S. Naval Cryptologic officer.

Well, welcome to the show, Mark.

Mark Weatherford: Hi Brian, great to be here.

Brian Contos: You know Mark, I know you're a very busy gentleman. We've been wanting to get you on the show for several months now. Maybe you could give our listening audience a little bit of background - of course, they've heard your bio - but a little bit of background of some of the types of things you're working on and maybe what's new in your world.

Mark Weatherford: Well, I've been a state CISO for... this is the fourth year; I've actually been here in California for about 11 months. I was the CISO in Colorado for three years previously under both Governor Owens and Governor Ritter. And so here in California... and it's interesting, I've been in the security business for a long time, wherever you go the problems are always the same it's just the scope of the problems are different.

Data Security within State Government with Mark Weatherford

So, here in California, prior to the recession we were considered the sixth largest economy in the world, and I don't know where we are right now, but it's probably not sixth any longer. But the scope here in California is pretty darn big.

We have around 143 state agencies, some additional boards and commissions and it's a very disparate environment from a technology perspective. So, we're all over the map with different kinds of technologies, different applications, appliances and networks and so it is a very heterogeneous environment as a nice way of saying it.

Probably the biggest challenge that I've had, the most important thing that I've been working on in the 11 months that I've been here is just trying to understand the environment, understand who the different organizations are, where they are in their levels of security maturity and then trying to figure out where I can be of best service to these different state agencies.

And state government, and again California is very similar to Colorado and similar to - I talked to my colleagues in other states - similar to other states, in that each of the different agencies really can be considered their own line of business.

The Department of Transportation is significantly different than the Department of Corrections. Their whole mission is different, their applications are different and it's different from a lot of the smaller boards and commissions.

So there are all levels of maturity within those organizations. Some of it is dependent on different types of funding that those state agencies receive, a lot of them have different compliance requirements which drive different types of... different levels of security maturity.

So, it's really a mixed bag in state government, but it is certainly the biggest challenge I've ever faced, trying to bring order to the chaos of state government.

Brian Contos: It's interesting, the order to the chaos, I work very closely with a number of your peers on the federal government side and they say every day is like herding cats. It's not so much a technical issue, it's not so much a political issue, it's just getting the right people, the right place, at the right time. That in itself can be just very trying. Obviously most of our listeners are somewhat familiar with what a non-state government CISO might do. What are some of the primary responsibilities that you have that perhaps differ from your colleagues perhaps on the commercial side?

Mark Weatherford: Well, there are probably a lot of things. One the... being a state entity is considerably different than being in the private sector. A lot of the processes take a lot more time. I have labor unions that I have to deal with on a number of issues; the procurement process can be cumbersome in state government. Just all of the different... the cultural issues of the large user base we have can be a challenge. They say that changing a culture is much harder than changing a technology and that's certainly true. So as we address new problems and new issues in state government, sometimes changing that culture can be a little bit difficult.

I'll give you one very, very recent example: as part of our response to the swine flu issue a couple weeks ago, I had already been working on a state-wide teleworks standard for users.

So we've been putting together a standards document for teleworking for security requirements and we'd begun bedding that with the state agencies and it's pretty amazing the responses that we're getting back. Some people are just saying, "Well, we can't do this,

it would stop us from being able to work, if we had to have a secure connection between a remote user and our network."

So the mindset of that is... my immediate response is to say, "Wait a minute. Do you understand what you just said? What you just said is you want to have unsecured connections to your internal network. Does that make sense to you?"

So overcoming some of those kinds of things, and not being able to make the rapid change that you can make in the private sector is probably the biggest challenge I have.

Sometimes it takes me months of, as I call it, coercion and hand holding to bring people to the point where they understand and agree to do things. Whereas in the private sector, when I have a security problem, or security issue, I just shoot it, kill it, and move on. So, it just takes a little bit longer sometimes to address security issues.

Brian Contos: Yeah. Boy, I imagine a state like California turns like a battleship stuck in mud sometimes, trying to get through all that. I've seen large organizations on the private side that have several levels to go through, working with the unions and things like that, but I also know dealing with the state, just the magnitude of the decisions affect so many departments, and the approval process, and things like that can be extremely lengthy.

When we're talking to financial organizations, healthcare organizations, retail, we commonly talk about things like Sarbanes-Oxley, PCI, and HIPAA. Are those things that you are concerned with as well, and are the other similar regulations that you must address as a state agency?

Mark Weatherford: Well, no. We're concerned about the same things. We have a number of health related organizations that have HIPAA compliance requirements just like the private sector does. We have a number of state agencies that conduct credit card transactions. In fact, they depend upon credit card transactions for their revenue.

We have essentially the same kinds of compliance requirements that the private sector does.

Even if you extend that out, California was the birthplace of Senate bill 1386, in I think 2003, on the data breach notification law. So, we are required, just like the private sector to investigate and notify citizens, and users, and businesses when we suffer a data breach.

So, my office actually, is the overall coordinator for security incidents. So, every incident that happens in state government gets reported to my office, and we work with the agencies to either notify if that's required, or mitigate if it isn't required, investigate, and again, do a lot of the hand holding and coercion to walk them through the incident response processes.

Brian Contos: So again, like you mentioned earlier, it's very similar. It just becomes a question of sheer scale. It just sounds like a number of different agencies across the entire state just make the complexity seem much larger. I went into this interview thinking... You know, I was going to ask you what threats you are most concerned with, but then you brought up things like swine flu. That got me thinking about business continuity, and disaster recovery.

What types of threats really do concern you? Is it really those that are cyber focused, or is it something else?

Mark Weatherford: You know, it's both. It's everything. I'm getting involved not as much as I'd like in some cases, and more than I'd want in some other cases in the critical infrastructure arena. Specific threats. We deal with the same kinds of things that everybody else does. Conficker was a big deal for us. You know, when you have a user base of over 200, 000 employees, that's not a trivial issue.

Then Conficker B came out in January, again working with them. Then working up to April first, just the constant reminders to the state agencies to stay patched. Actually, we had relatively few incidents and outbreaks of a Conficker virus.

You know, botnets. We get involved on a fairly regular basis. Some of our agencies outsource their web hosting to the private sector. We get notifications just like everybody else in the world, that we've got infected websites or infected hosts that are supported somewhere else. So we've got to work with private sector organizations sometimes to remediate and mitigate.

It's the same threats. I would say, the one maybe additional thing, while a lot of businesses and organizations are distributed, California's a big state. We've got offices and satellites all over the state. Everywhere from Tula Vista to Eureka.

It's a big state. There are Department of Motor Vehicle offices everywhere. There are tax offices. We have little offices all over the state, and a lot of those, their staff are relatively small. A lot of them are completely remotely managed.

You start thinking about things like park rangers, and water resource officers, and things like that, that is out in the field and very rarely come back to an office. How do you make sure that their systems are staying patched and up to date?

You know, there's a whole lot of hurdles there that state agencies have to deal with that some private sector organizations don't.

Brian Contos: Yeah, isn't that the truth? Especially when you start bringing things up like critical infrastructure. I was working with an organization not too long ago that works with the dams. When they're working with the dam systems, they have what they call "ruggedized firewalls," which you're probably familiar with, that are sitting out in some shack somewhere preventing... Literally, they're concerned about snakes and spiders more than hackers in these little shacks.

They're unmanned shacks that collect data, and send and report it back. There are thousands of these things all over the country, just collecting this data and pulling it in. It can be just a monster to try to manage and maintain, and a state the size of California I could just imagine.

Let me ask you this, and maybe this is something that you can't talk about, but if you can, that would be great. I've done a lot of work with some organizations that, after 9/11, they've started putting together fusion centers.

There was this discussion following 9/11 that there wasn't enough communication between state and federal agencies, federal to other federal agencies, local law enforcement, et cetera.

So, New York for example, they put together an intelligence agency... New York State put together their own intelligence agency, with agents worldwide, et cetera. Their actually

Data Security within State Government with Mark Weatherford

doing intelligence gathering now, not just simple receiving of intelligence from FBI, CIA, NSA, and other sources. Then New York metro decided they wanted their own as well.

Then you're in a situation where you had all the federal agencies, you had state agencies, the New York State agency, and New York Metro all getting their own information, and not just being consumers of information, and having to share amongst the various departments.

Is that something California does as well? Is that something we either do or we are looking at doing? And if we are, how has that progressed over the years?

Mark Weatherford: Well I will say that is one of the nuts that I haven't quite cracked yet. We do have a fusion center within state government, and we have some cyber analysts that attach to that. Most of them have securities clearances so they are able to receive and share information with the Feds. We work fairly closely with the FBI and other law enforcement organizations.

While my focus is, I would say, 95% on Sacramento, because that is where state government resides, California is a big state, and we work with some of the different FBI field offices up and down the state.

The InfraGuard organization; most of us are members of InfraGuard. So we do have...We have, I would say, a fairly robust information sharing with the existing organizations.

We work with... The Multistate Information Sharing and Analysis Center is actually hosted out of New York. But every state CISO is a participant in that. They are closer to the line with US Cert.

So we get... I mean I have received a couple of advisories already this morning from the MSI on specific kinds of things. And we share information back and forth with other sates as other states are seeing certain types of activity or incidents. We share that kind of information.

So it allows a little bit of coordination at the state government level for sharing that. One of the things I don't think that any state has done a real good job at yet is coordinating with local governments.

And it is a little bit of challenge in a state as large as California just to know who in the heck to talk to sometimes. And sometimes we get advised of events or incidents in local governments and we need to go find somebody that has got a website hacked or perhaps a comprised network. And sometimes it takes a day or two just to track down the right person who owns that.

That is not endemic to California. I had the same issue in Colorado, and some of my colleagues in other states have the same issue. There is really no good way, at least that I have been able to figure yet. So maybe if any of your listeners know how to help me, I would be happy to talk to them.

But there is no good way to bring together all local governments, at the county, city, local borough levels, to just have that coordination piece. What we do, essentially, as we do talk to people, we add people to our email list so that they can be on distribution. We keep a master list of who is who throughout the state that if we need to we can get a hold of them.

Brian Contos: Yeah, it is interesting. It is that whole issue of who to tell, how to tell them, when to tell them, and how much information to give them. It seems to be an issue with

every organization that is trying to deal with fusion centers today. I don't know if there an easy answer to that at all, but I know it is something that everyone is grappling with at this point. As we wrap up here and you look into your information security crystal ball, how do you see things evolving? How do you see information security evolving, and perhaps how do you see the threat-scape in general evolving?

Mark Weatherford: I am not going to say anything profound here I don't think. But we have migrated from worrying about our networks to worrying about our data. We need to holistically, as a nation, as a state, as a business, we need to understand that the data is the issue now and it is not a lot of the peripheral stuff. While we still need to maintain a solid perimeter, there are a lot of other moving parts that we need to be thinking about and that we need to be worried about now, because people are after our data. Anyone who thinks that they are immune to that, they are going to be the victims.

So I would say the laws are changing. The laws are starting to see some more severe penalties for some of the cyber activity, which hopefully is going to have some impact.

There is a lot of media information now about how, because of the economy, that we may be seeing more insider related activity. And while I don't have anecdotal evidence of that in state government, that makes sense.

So I think we do need to be paying more attention to what is happening inside our organizations without letting our guard down for what is happening outside of our organizations.

Brian Contos: Well put. When it comes down to sensitive data, the way you protect it typically... I am even finding that the term insider is losing meaning just because so much data is digitized. Access is much, much grander than ever before. Partners, consultants, contractors, other agencies, whomever can get access to a lot more data a lot quicker and a lot easier than ever before. Like you said, sensitive data is the target. Auditors audit it. Bad guys go after it. And we have to protect it. And I am right with you. I think that is probably one of the core issues for any organization for the next few years.

Mark Weatherford: We say that having a perimeter is important. But you know what? Because of the whole social networking environment and the Web 2.0 environment, the perimeter is not there anymore. We don't really have a perimeter anymore. Our perimeter is Port 80. It is not anything to bury our head in the sand or go screaming from the roof about, but it is something we need to address head on. We just need to pay attention to it.

Brian Contos: Well Mark, I want to thank you so much for joining us on today's podcast.

Mark Weatherford: Thank you Brian. Good talking with you.

Brian Contos: If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.



North America Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

International Headquarters
125 Menachem Begin Street
Tel Aviv 67010
Israel
Tel: +972-3-684-0100
Fax: +972-3-684-0200