A city is vastly different from a commercial company. We wanted to learn if a city CISO needs to be similarly different to a private sector CISO. *SecurityWeek* spoke to two city CISOs, from the City of Tampa, and from Tallahassee.

Martin Zinaich heads cybersecurity at Tampa – the 47th city in the U.S., with a population of more than 404,500. Technically he is Information Security Officer; but in practice he is Tampa's CISO. He has held his position since 2001, making him one of the longest serving security leaders we have spoken to.

Thomas Vaughn is CISO at the city of Tallahassee, a much smaller city ranked at 125th in the country with a population of just under 200,000. Vaughn was recruited to the position in 2020 to expand and improve the city's security posture. Prior to this position he had been CISO for the State of Florida.

The difference between a city CISO and a commercial company CISO

The fundamental difference between a city and a private sector company is the multiple and quite different lines of business in a city. A commercial company may have two or three lines of business, but a city has many. "We have our public safety, our police department, our fire department, the parks department, the water department, wastewater, refuse, energy, traffic… all those are different lines of business. And while there's some

economy of scale in all that, it's drastically different in technology," comments Zinaich.

Vaughn agrees with this, adding there is a basic difference between a private sector CISO and a government CISO. "When you talk about a government entity like a city, it is different because there is such a broad range of different operations - business operations where we operate. That's a key difference."

It is the effect of these multiple lines that differentiates the jobs. Zinaich does not have different cybersecurity teams for the different lines of business; "and that makes it tough, because each security engineer has to cover so much. You have to be comfortable juggling a lot of balls a lot of the time, with a lot of interruptions in your strategic plan while you take care of some tactical needs."

It is slightly different in Tallahassee, but that is more for accidental historical reasons than current design. "The security program here is relatively new," said Vaughn, "and there are aspects of cyber that were already being performed by individual departments. A good example of that is Electricity - we have two power plants, and we produce our own electricity. Those power plants obviously have federal requirements – such as FERC– in the United States, that had to be performed, and had to be maintained by someone. So, the electric utility developed its own capability for that; and that was prior to me having an overarching security program. So, yes, in Tallahassee, there is some separation, there are a few separate teams, but I think that that was more accidental than intentional, and I think that over time those things will merge together."

Budget always has a defining role in what can and cannot be done in security. We asked if there is a difference in budget between the private sector and cities. "Oh, absolutely," said Vaughn. "It's a little more nuanced, because larger cities tend to have better budgets. And in the private sector, it depends a lot on which part of the private sector you're in. If you're in the financial sector, you tend to have more funding because there's a lot more compliance requirements. If you look at something like, say, a construction firm, you probably wouldn't have similar funding for cyber, because there aren't really any compliance requirements. So, a lot of the spending in the private sector is driven by compliance."

He explained further that while budgets in the private sector vary by sector, all cities tend to have similar compliance issues, so the budgets are often tied to a percentage of the IT budget – which is why bigger cities tend to have bigger budgets.

Personal attributes and advice

Given the difference between the role of the city CISO and a private sector CISO, we asked what personal attributes best serve the City CISO. “For me, there are two attributes,” said Zinaich: “patience and integrity. If you come from a role with a single line of business and are then faced with these multiple lines, there’s going to be some frustration just in the sheer magnitude of trying to do things. Something that might be simple in a single line of business, when you ratchet that out to all the different lines, you run up against some things you hadn't even thought of. So, patience and working with integrity with people is a big deal.”

Vaughn absolutely agrees on patience. “It is the hardest thing for a security guy, but we have to be very patient in the work we do, especially at the city level. Resources are minimal, and the work is so broad. We must accept that some things can't get done, or some things may not get done as soon as we'd like. So, it requires a lot of patience.”

He added that diplomacy is also important. “The ability to be diplomatic and to compromise when it's necessary is important for someone doing CISO work at the city. We may have security requirements that we can't meet. So then, as a CISO we have to say, how close can we get? What's acceptable? And that requires a lot of compromise, and some security guys don't have that. Some security folks are very much black and white. And I don't think you can be that way in a city environment.”

However, despite some city-specific attribute requirements, neither of our CISOs think it would be difficult for an existing CISO to move from the private sector to the city environment, nor vice versa.

We asked both what was the best advice they ever received in their own personal journeys. “It was that things change,” said Vaughn. “Things always change, and change is something we need to embrace. We cannot secure things one way today and expect them to remain secure tomorrow. So, we must be flexible and open-minded and embrace change as part of what we

do. If I hadn’t been told that and understood it, my life as a CISO would have been much more difficult.”

The best advice Zinaich has received was to ask one simple question: ‘How do you know that?’ “A lot of times we make an assumption when we’re troubleshooting or protecting something, or when we’re auditing. So, I ask myself, how do I know that? It has become the best troubleshooting tool I ever use. When I think I’ve got something covered, how do I know that?”

The other side of the advice coin is what advice would they give to new, potential security leaders. Zinaich advises patience, integrity, and empathy. “You’re not going to conquer the mountain as soon as you think you will; so, patience is key,” he said. “Then personal integrity – you need to make sure that everyone trusts you. Finally, empathy – you must really understand what the business is trying to get done. If we made everything so secure that nobody could log in, it would be great; but then… there wouldn't be any business.”

Vaughn’s advice is to value diversity. “By that I mean not just diversity in your staff, but diversity in yourself. Diversity in your program, because security in a vacuum is never as effective as security that considers everything that is happening around it. But also in your staff. People who do security work need to have expertise and knowledge in other fields. I had a young lady who was sort of my policy person. She had a law degree. Didn't have very much cyber experience, but she was very good at what she did. Her knowledge set outside of regular cybersecurity stuff made a real difference. I had another gentleman working for me who had a master's degree in Theology and had been a priest for a time. He brought valuable things to the table because he knew how to talk to people, he knew how to negotiate, and to listen. Those skills were vital to the work – but they weren't necessarily cyber skills.”

Reporting upwards

Having a budget as a percentage of IT spend implies that the CISO reports to the CIO. This is the case for both of our city CISOs – and they both have somewhat ambivalent attitudes towards this. Zinaich comments, “It works if you have a good working relationship with the CIO.” He accepts that a lot of organizations are trying to move the CISO from under the CIO, but adds, “That has its drawbacks too, because you almost need to be embedded with the technology to make sure it gets rolled out properly.”

Vaughn believes that in his own situation, it wouldn't be realistic to have him report directly to senior management. "The security program here is very immature – it's very new, and I was hired to build the security program. Because of that, expecting my role to be separate and apart, and to report directly to top level leadership seems unrealistic. When you're in a program that's still being built, it's unproven, there's no established confidence, and you're not well known. It just doesn't make sense. So, the answer really is something you hear a lot from security people: it depends. Ideally, the CISO should be separate from the CIO, but we're not always safe to do that."

But while Zinaich has pointed to a synergistic value in having a close relationship between CIO and CISO, Vaughn is clear on the potential for a conflict of interest between the two roles. "I think it's inherent. I think a conflict of interest always exists, so it's not even a question of there may be a conflict of interest, there is a conflict of interest, and it happens every day. I think the only way that such conflicts can operate, and we can still get work done, is when the relationship between the CIO and the CISO is strong. Unfortunately, that depends a lot on personalities, and I think that goes to the root of the problem."

Responsibility downwards - protecting the citizens

Both CISOs accept a responsibility toward the citizens of their city. Zinaich says his function is to protect the services that the citizens use and rely on, and to ensure those services are not impacted.

Vaughn is more expansive. "I do have a responsibility, but the requirements have mostly been identified by me. When the city thought about developing a cyber program, I don't think they really understood what that meant. Now that I'm in place, I've identified a lot of areas where the things that we're doing directly impact the data that belongs to our citizens. So, daily, I'm thinking about how some action we take will benefit the citizens and protect their data. When we're doing security stuff, I often relate it to the impact on citizens, because for me that's the bottom line. That essentially is our business – taking care of citizens. So, anything I do to secure systems and data, ultimately ties back to citizens. The city didn't realize that's what they were hiring me to do, but I'm very much making that the case."

Zinaich added, "I never forget that people's tax money is being used to do what we need to do. We're in the business of supplying services – police,

fire, water, parks, traffic – and we have to do that as best we can with the least amount of cost."

Certifications

Zinaich has at least seven security certifications – certainly, all the major ones. Vaughn has 'just' three. It could be expected that certifications for employment candidates would be more important to Zinaich than Vaughn; but that isn't necessarily so.

Talking about the importance of certifications in recruitment, Zinaich commented, "It's not all that important to me. If I had a candidate that had built his own lab and was very good at this, I could care little about his certifications. I usually like to see at least one to make sure the candidate had some formal training; but that's not important. It's not real high on my list."

Vaughn said he makes little of the three certifications he has, "because I don't want to be identified by my certs – I want to be identified by what I actually produce." Despite this, he added, "I do believe that when I'm hiring someone, those things matter. Because if I have someone who's a CISSP that's applying for a position and I have someone who's not, I'm gonna tend to lean towards the CISSP because I know there's a baseline of knowledge. I think that's the best thing about a cert – it tells me that there is a baseline of knowledge, and I sort of know what I'm getting."

But he added, "I don't specifically require certs when I recruit personnel. Those things matter, but I don't want to make them too firm a requirement. There are plenty of people out there who are good at cyber that don't have those kinds of certs, and sometimes, sometimes, you have to recognize that."

Vaughn believes that 'passion' is the most important attribute when hiring – but added a caveat. The candidate also needs to demonstrate aptitude. "It's not just about passion, it's also about having the ability to learn. I often say I would rather have someone with a positive attitude and a strong work ethic over someone who's highly experienced without those things. Essentially, I feel that I can train someone with the right attitude and motivation. But someone who doesn't have those things is very hard to work with, regardless of experience."

The importance of certifications seems to be as much in the ability to gain them than it is in the knowledge they demonstrate.

Professionalizing the cybersecurity industry

Certification leads directly into a subject that has interested Zinaich for many years – and one that I have discussed with him several times over the last decade: the desirability of professionalizing the cybersecurity practitioner industry.

In 2015, Zinaich wrote an almost seminal paper on the subject: What does Information Security have in common with Eastern Air Lines Flight 401? It uses a simple metaphor. In 1972, Eastern Air Lines Flight 401 crashed in the Florida Everglades with 101 fatalities. It appears that the crew had become fixated on a burnt-out nose gear indicator. While focused on something that was not in itself catastrophic, the crew failed to notice that the aircraft had moved into a long, slow, automated descent – which continued until the aircraft crashed.

Zinaich's concern is that without proper governance of cybersecurity practitioners, cybersecurity itself will follow a long, slow descent into catastrophe.

Few will disagree with the premise that professionalization would be anything but beneficial. Zinaich uses the example of the medical profession model. The only problem is who should instigate and control the governing body, and therefore control who and how people can enter the profession. The option is effectively between the cybersecurity industry itself or the government.

In 2018, Zinaich told *SecurityWeek*, "The idea that such critical ubiquitous lifeblood like technology, the internet and IoT will not be regulated heavily, as each new breach expands its impact, is very short sighted. We either lead this effort or get lead."

The only difference now is that Zinaich believes the opportunity for the practitioners to develop their own professional body has passed. "It's going to have to come from regulation," he said.

But if regulation comes from the government, will it evolve into something like the current data protection and privacy laws, with each state having

slightly different regulations – or could the federal government impose federal regulations across the entire country?

"No," said Zinaich; "not unless it turns into a totalitarian regime. What they'll do is what they've done before: if you want to sell to the government, you will need to meet these criteria. And that's a big driver." What the federal government could do now, of course, is impose its regulations on all federal agencies and departments.

We can see a model for this latter route being played out in the UK today, which has the political advantage of a central government with almost total political control over the whole country. The NCSC, which is part of the government GCHQ spy agency, has a program called Active Cyber Defense. Within this there is something called Protective DNS (PDNS). Participating organizations – which already include most government departments and a growing number of NHS organizations, pass all outgoing traffic through the PDNS system which checks it for indicators of compromise and malicious IP destinations.

If the scale issues can be solved, there is little reason for this program not to be expanded across the whole private sector.

There is an excellent security – especially 'national security' – argument for this program. Until you remember that the NCSC is part of GCHQ. There is little pushback against the NCSC doing this – but there would be greater pushback if people more directly associated PDNS with GCHQ rather than NCSC, and that the program involves voluntarily giving the agencies one's entire browsing history.

Incidentally, on May 25, 2021, the grand chamber of the European court of human rights ruled that GCHQ's mass collection of communications revealed in Edward Snowden's disclosures was indeed illegal. Having people voluntarily hand over their data rather than having to steal it would seem an excellent alternative for GCHQ.

Vaughn has a slightly different take on professionalization. He agrees with it in general terms, but wonders whether it is necessary or even the right approach. "I believe that security is becoming so ingrained in everything else we do – not just in IT but in society in general – that I question whether strong professionalization in something very specific like cybersecurity will make sense in the future," he said.

“What I mean is we cyber folks are going to be very much embedded with everything else we do in society. It’s going to be everyone's role to do cybersecurity work, whether they're cyber folks or not. So, sometimes by professionalizing something a lot, you create separation. And I don't know that's the best path forward for the future. I wonder sometimes, if integrating cyber into all our thinking, and making it more of a natural part of our jobs makes more sense. Would professionalization hurt that? I don't know.”

Future threats

The last thing we ask our CISOs is where they think future threats to their sector will come. Zinaich sees it coming from two directions – from the increasing sophistication of the attacker, and the cloud-induced sprawl of the business. “It used to be just zero-days and ransomware, BEC and standard data breaches,” he said. “But now we’ve also got state-sponsored actors going after our supply chains.”

And then there’s the cloud. “As we moved more business to the cloud, the hoped-for reduction in risk and resource demand simply hasn’t happened. The shared responsibility model helps a bit with the hardware and patching the base underlines, but it still leaves an awful lot for the CISO to cover. Shadow IT, which we worked hard to eliminate, is growing again. And with the configuration, usage, tracking, visibility – there’s all that stuff we now have to do on top of everything else we do.”

Vaughn is also concerned about nation states attacking the supply chain. “They are actively targeting government infrastructure,” he said. “When you look at things like SolarWinds and Exchange and Pulse, we have nation states that are actively using our own tools against us. As a small government organization, we don’t have the resources to deal with those issues. When you think about supply chain risk, we don't have the capability to be able to vet our supply chain. That's a serious challenge, and it will be, for years.”