onlineeducation.com

Interview with Martin Zinaich, Information Security Officer, City of Tampa

22-28 minutes

About Martin Zinaich

Martin Zinaich is the Information Security Officer for the City of Tampa's Technology and Innovation Department. He created an information security office for the City of Tampa, installed and maintains the city's vulnerability assessment services, and instituted an end-user awareness education program for city employees. Previously, Mr. Zinaich worked for fifteen years in the private sector, as a research and development engineer and a technical manager in the telecom industry. His areas of expertise included video encryption and decryption, as well as designing discrete RF and digital circuits.

Mr. Zinaich has written articles for *Popular Communications*,

Network World, and *Novell Research AppNotes*. He holds a Bachelor's of Science degree in Information Technology from the University of South Florida, a Bachelor's of Science in Business Administration from Chadwick University, and an Associate of Science in Electronics Technology from Hillsborough Community College. His professional credentials include a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Security Auditor (CISA), Certified in Risk and Information Systems Control (CRISC), Certified Security Software Lifecycle Professional (CSSLP), and Certified Ethical Hacker (CEH). Mr. Zinaich is the author of "What does Information Security have in common with Eastern Airlines Fight 401."

Interview Questions

[OnlineEducation.com] Is there a typical workday for an information security officer? More specifically, what are some of your primary concerns on a day-to-day basis, and how do you prioritize your responsibilities?

[Mr. Zinaich] The first item to understand about information security/cybersecurity is there is no "typical" day. Primarily, this is because there is no prototypical information security office. This nascent industry is still searching for its footing. So, an emblematic day is actually based on a few factors, such as your industry vertical, your reporting structure, the size of your organization, and if your organization is pre-breach or post-breach. I often touch on that last item when speaking on the topic of cybersecurity. The information security office often looks very different post-breach because the business then engages cybersecurity as a business

imperative and not just as a technology eccentricity.

In a pre-breach organization, a practitioner focuses more on the “A” of the “CIA” triad — availability. This may entail firewalls, proxy servers, certificate authorities, directory services, and providing a lot of third-tier troubleshooting. Everyone blames the firewall for availability issues. If you are of the “business enabling” cybersecurity mindset, which I am, you often use your skills to help solve access and firewall problems, even if they are not in your purview. At the same time, you will be trying to “sell” the information security program.

In a post-breach organization, a practitioner will be focused more on the “C” and “I” of the “CIA” triad — confidentiality and integrity. This may entail security incident and event management, threat intel feeds, pinpoint log reviews, and focusing on policy and business integration. The latter can now happen because the business is engaged at the proper level. You are also likely to have enough staff to employ dedicated tasking. No more “selling” at this stage; the business is now asking the right questions.

Add to this mix your business vertical. I commissioned a survey through *Wisegate* to poll fellow Chief Information Security Officers (CISOs) to understand their business coverage, their staffing ratios, and their percent of budget numbers. The results match the same numbers I pulled from analysis conducted by Gartner Research. In essence, how engaged, focused, staffed, and funded a security office is can be directly related to the industry. If you are part of a financial organization or three-letter government agency, you are going to feel a lot better about your resources. If you are in the education profession or local government, expect to feel more frustration than your counterparts do.

[OnlineEducation.com] When it comes to communicating security concerns to other members of an organization in a proactive way, specifically in the pre-breach, non-crisis phase, what are some of the strategies that have worked for you? Do you have an example of a situation in which you've accomplished this effectively, or in which a breakdown in that chain of communication has led to bigger problems?

[Mr. Zinaich] One creative thing I did was to produce a one-hour video of myself doing white-hat hacking into the organization I was working for. It showed the system vulnerabilities and how I was able to exploit weaknesses and take control of critical systems. That was shown to the CIO, who then wanted the entire IT staff to watch it in an all staff meeting. That really changed the mindset of the IT staff. They quickly started taking security more seriously as a business imperative. Next I shared it with the internal auditor. He put it in an audit report, and requested that it be viewed by all senior staff. I edited it down to 15 minutes and we had our first "security at the table" moment. I came away with our initial Information Security Charter and a direction from the business.

Of course, I've seen the flip side. A peer once pushed for her security office to control all social media accounts, which would encompass configuring passwords, rotating them, and providing access through managed accounts. It was a very routine and simple request, but it didn't fly. Then, one day a department called her in a panic: "Our social media person has gone missing; we need to kill the Facebook account ASAP!" Unfortunately, there is no simple and straightforward way to get control back of a Facebook account when you don't have access to the account. Good governance would have prevented that crisis from happening.

[OnlineEducation.com] From your perspective, having worked in the private and now the public sector, how different and/or similar are the information security concerns and protocols from industry to industry? In other words, are cities like Tampa essentially dealing with the same cybersecurity issues as a manufacturing plant, a bank, an insurance company, or are they quite different?

[Mr. Zinaich] When I worked in the private sector, the term cybersecurity was yet to be invented. If business years are like dog years, cybersecurity is still a very young puppy. The question is interesting in so much as, like cybersecurity, the difference between public sector and private sector has less to do with the technology and more to do with the organic nature of an organization. A CEO change is very much like an elected administration change. All leaders inject a life, image, and direction into an organization either explicitly or implicitly.

When I worked in the private sector, I was lucky enough to attend a Malcolm Baldrige National Quality Award ceremony. Established by Congress in 1987 for manufacturers, service businesses, and small businesses, the Baldrige Award was designed to raise awareness of quality management and recognize U.S. companies that have implemented successful quality-management systems. The ceremony included a video of all past leaders commenting on what got their organizations to that level of accomplishment. A theme started to coalesce as leader after leader noted what they believed got them there. They all seemed to say in some fashion, no matter your position in the company, everyone knows what our main objective is and they are focused on it.

The private sector companies I worked for usually had just one or

two primary lines of business. From a security standpoint that really helps narrow the scope. Local governments, on the other hand, have a multitude of business lines. For example, a city is a police department, a fire department, a water department, a waste water department, a traffic department, to name just a few of its components. Therefore, the resources-to-coverage formulas are usually upside-down. One of the best ways to handle limited resources in cybersecurity is to target the organizations most critical systems and flows. However, when you have a multitude of business lines and each has critical systems, regulations, and "wants," this quickly becomes a daunting task.

I always thought it curious that the Baldrige Award did not have a "government" category until 2007, when a government and nonprofit category was added. The 2015–2016 Baldrige Excellence Framework includes dealing with data analytics, data integrity, and cybersecurity. Baldrige even has state, local, and regional awards programs. However, it doesn't seem to have the same traction in the public sector that I have seen in the private sector. The last local government program of this type I was asked to participate in (I am excluding the name on purpose) did not even have a cybersecurity category.

It may seem strange to see an information security practitioner talk so much about business; however I feel that is where this profession is missing the mark. You cannot function from a small corner of the IT department and affect the kinds of change required to protect a business in this new digital age. Technology is ubiquitous to businesses. It's an essential lifeblood. It should be treated as such.

[OnlineEducation.com] As someone who has a CISSP

certification, as well CISM, CISA, and CRISC certifications, what kinds of coursework and practical training would you recommend that students look for in an advanced degree in cyber security? What kinds of experience outside of the classroom are helpful in cultivating expertise in the field? And, how important are those certifications?

[Mr. Zinaich] When I sought my first and second certification in information security, higher education was not teaching this discipline. Certifications carried a lot of weight because they were one of the only formal ways to get educated in this career path. But, I fear infosec certifications are becoming the modern day equivalent of the Novell Certified Netware Engineer (CNE) and the Microsoft Certified Professional (MCP). Each started out with the purest of intent, making sure the practitioner understood the technology. They soon turned into a business, with tons of quick-study and fast-pass options. The term “Paper CNE” was soon being coined to describe those that simply studied to pass a test but did not have the practical knowledge.

Having said that, certifications do expose practitioners to areas of coverage that might otherwise be overlooked, because information security is still trying to define itself in business. My best advice is to have at least one certification. If you know the area of coverage you are most interested in, find a certification covering that space. The certifications have much overlap but can be very distinct. For example, the CISSP (the known gold standard) is often described as a “mile wide and inch deep.” The CISM, on the other hand, focuses on information security integration into the business. When you understand the organizations behind each certification, it becomes clear they have different targeted goals. Moreover, that

may be the best part of a certification — the organization behind it. Once you are a member (and you don't always have to be certified to be a member) you have access to great articles and forums that help bolster your continued career growth.

As to practical experience, one of the greatest options in IT and IT security is the ability to have your own lab. With the cheap cost of used routers, firewalls, and switches, and the ability to do a lot of this in a virtualized environment, having your own lab to experiment, test, validate, and learn is extremely helpful. The key to being effective in any career is truly understanding that basis of what and why, not just knowing the answers for a test. As a CISA, I believe the five most powerful words for an auditor are the same for any information security professional — "How do you know that?" In information security, you are going to be presented with numerous challenges, everything from business integration to the "noise" of telemetry data. In each case, you will need to be able to adjust to the environment and understand what you are looking at and how it relates to the end goal.

[OnlineEducation.com] The popular conception is that cyber attacks are a constant threat and that there will always be another breach or vulnerability to address. Is that an accurate portrayal of the reality? If so, how do information defenders stay sane, prioritize, and act appropriately? Are people on the front lines of this battle going to have to accept a certain amount of chaos as the norm?

[Mr. Zinaich] This is another great topic. When I started in this business and information security was just starting to be mentioned in IT shops (note: it still is rare to hear it at the board level) there was a term used to help sell information security — FUD (Fear,

Uncertainty, and Doubt). I never liked that tactic, and I never used it. I know the boy who cried wolf story, so it seemed silly to base a program on FUD. However, you had a perfect storm brewing with the addition of personal computers and the Internet. Soon, FUD was not a tactic; it was a reality. Because business still kept information security contained to a corner of IT, the products they made, the business processes they ignored, and the lack of integration all combined to create the disorder we currently call business as usual.

Until there is an integration of information security into the business proper, yes we are going to live in a breach-a-day environment. Moreover, as the Internet of Things (IoT) looms on the near horizon it will only get worse. That was not my position many years ago, but time has proven the direction is not slowing.

This is a topic dear to my heart. Having lived this business for so many years and watching the paradigm shift in organizations from secure business practices to the want of the moment, I have spent many a night conversing with frustrated colleagues. I coined a term called the “institutional attack vector.” We do not battle just with flawed protocols, poor coding, third party integrations, script kiddies, and professional criminals — we too often have to battle with the organization we are trying to protect.

I wrote a multipart article on this topic called “What does Information Security have in common with Eastern Airlines Fight 401.” In the article, I explain how we got to this point and suggest how professionalizing this industry may just be the best solution to elevate information security to the proper level across all business verticals.

[OnlineEducation.com] One of the major concerns you've written about and commented on is the need to create a bridge between information governance and cyber security within an organization? What does someone entering the field of cybersecurity need to know about the organizational structure of IT departments and how cyber security fits into the larger picture of systems and data management?

[Mr. Zinaich] Understanding the organizational structure of IT and how cybersecurity fits into the larger picture is key to being successful. The Information Systems Audit and Control Association (ISACA) often emphasizes the "tone at the top" and "risk appetite" in an organization. The National Association of Corporate Directors (NACD) also talks about "risk appetite" and integration of cybersecurity into the business proper. The major problem is business leaders are not reading ISACA material nor NACD findings (albeit the latter comes as somewhat of a surprise to me). Therefore, practitioners very much need to understand their environment and understand where and when gentle pushes might be made to get traction. They also need to understand the business goals and see how they might help enable those business goals. This is one reason I elected to get degrees in both business and IT versus one master's in information security. With the number of infosec certifications I carry, I thought it would be more helpful to know more about how the business side of an organization thinks and works. And, just as business can lack an infosec vision, cybersecurity can be lacking a business vision.

In the past, my teams have actually taken on operational projects from corporate WiFi to managed file transfer systems, simply to put in place the secure foundations that the business needed and can

then build upon. That kind of pro-business integration also comes at a cost to the information security program. You are giving up resources to help the business, but there may not be an understanding that you have just lessened your time on task with security in hopes of limiting exposure in foundations. The risk is this can quickly become “business as expected.”

Governance is also key, but it is also rare. I recently spoke at an auditor convention where I asked, “How many of your organizations have an information security charter?” One hand went up. I then asked, “How many of your organizations have an audit charter?” Every hand in the room went up, and then a bunch of laughter. I guess I effectively made my point.

[OnlineEducation.com] Given that reality, what are some of the best ways that cybersecurity professionals can communicate security concerns within an organization?

[Mr. Zinaich] This goes back to that ISACA idea of “tone at the top.” Short of a major breach, there is nothing that is going to make an organization listen if they do not recognize the risk. If they consider cybersecurity to be just an IT issue, it becomes a Sisyphean task. Doing that little video I mentioned earlier helped open a lot of eyes. Encouraging leaders to attend conferences or gatherings where technical business risk is discussed can help. When they see their peers creating charters and instituting formal governance they begin to see that other companies have a holistic view of cybersecurity, and it’s usually something they want to emulate. Sharing articles from ISACA and ICS2 can also help. The NACD is also a good resource. They have a publication that deals specifically with business and information security. Because this is coming from an organization of “Corporate Directors” and not a

techno-nerd publication, it has more weight in the eyes of business leaders.

[OnlineEducation.com] Can you elaborate on the role of governance in cybersecurity, and what cybersecurity professionals should know about governance. What should an information security charter incorporate?

[Mr. Zinaich] Security governance is having all the right players making business decisions that reach across an organization regarding technical risk. In my opinion, businesses have lost sight of the reach of and reliance on technology. So much of what a business does now depends on technology. So, it's important to know who controls social media platforms for an organization, and who speaks for that organization on social media. Is there an off-boarding process that handles all user technology touch-points? What compliance issues reach across the organization and who owns those processes, including a legal point of view. Is remote access ad-hoc? Who approves access to which systems remotely, or is everything available? What about BYOD? Are there legal issues if employees are encouraged or required to check email off-hours? These are important questions for information security and governance.

In December of 2015, a federal judge ruled against a group of Chicago police officers who claimed unwritten rules discouraged them from filing for overtime for off-duty work performed on their BlackBerrys. In the ruling, U.S. Magistrate Judge Sidney Schenkier said the city has an established procedure for filing overtime and did nothing to prevent officers from using it. In essence, the ruling indicated that officers should be paid overtime for checking email. In fact, Paul Geiger, one of the attorneys representing the plaintiffs,

said that, “The only good news here is that all officers can be paid for off-duty BlackBerry work going forward even though a police department’s general order says precisely the opposite.” This is a classic illustration of how pervasive this technology has become in the absence of normal business planning and foresight.

As to a security charter, first and foremost it’s a statement that information security is a real and pressing concern for the entire business. And, it gives the security office and security officers the authority they need to do their job. Charters should be small — just one or two pages. They should state the purpose, specifying that the business relies on technology and how a lack of security in that area could impact the business. It should point out how everyone in the organization would be affected. And, it should create a point person for security concerns, preferably a CISO.

Once there is a designated CISO, an organization should define the role and responsibilities of that person. There should be a security governance group, with members from various departments, and in larger organizations you want to have security coordinators to act as liaisons, training and updating employees as extensions of the security office. In a well set-up organization, you should also have information owners, who have responsibility for the data in systems, and system owners, who are responsible for the hardware, operating systems, databases, and applications. And, in the event of a breach, there should be an emergency response team, with designated members who have designated roles; including handling the public relations side of a cybersecurity situation.

Most importantly, the security charter should be signed by the CEO and communicated from the highest corporate executive in the business, to emphasize its importance. A short charter with just a

few small sections sets out the framework to communicate that the business is engaged in cybersecurity, is aware of the digital risk landscape, and is doing due diligence. It defines authority and responsibilities for information security and assurance, and it lays the foundation on which further policies and procedures will rest.

[OnlineEducation.com] You've also written about and commented on the challenges information security specialists face in managing the faults unintentionally built into commercial operating systems and applications, like software that isn't set up to work through a secure proxy server. What is the best way for experts in the field stay up to date with glitches in new software and network systems, and with new cyber attack modes and strategies?

[Mr. Zinaich] Staying in tune with current cybersecurity risks and exposures can be formidable. If you are currently working in a business, find information security groups representing that area of coverage and join them. If your area is too new or off the beaten path, start one. With the virtual world as it is, creating a group on LinkedIn is a good option. However, make sure there are not already established groups.

As noted earlier, the certification industries are also good resources, groups like ISACA, ISC2, NIST, SANS, EC Council, etc… I happen to be a founding member of *Wisegate*, and find it a valuable resource. The options do not just stop there; one can remain well plugged into the cybersecurity ecosphere without joining anything. Get a good RSS aggregator and start looking for infosec feeds. Some of my favorites are *SecurityNewsPortal*, *Securityintelligence*, *CSO Online*, *DarkNet*, *Dark Reading*, *Krebs on Security*, *US Cert*, *SC Magazine*, *Hak5*, *DatabreachToday*, *SANS*

Internet Storm Center… The list goes on and on, just like the risks.