Cyber Safe Cities Podcast

Incident Response Preparedness with Wadeed Mian, Vice President of Digital Forensics and Incident Response with ISA Cybersecurity

[00:00:00] **Tenielle Bogdan:** Welcome to the Cyber Safe Cities Podcast. This podcast is brought to you by the Municipal Cybersecurity Best Practices Initiative led by TECHNATION Canada and funded in part by Public Safety Canada under its cybersecurity cooperation program. This podcast looks at the ways Canadian municipalities can ensure they are cyber safe. To learn more, head to technationcanada.com and check out our Municipal Cybersecurity Best Practices Guidelines.

I'm your host, Tenielle Bogdan. And today we are chatting with Wadeed Main, Vice President of Digital Forensics and Incident Response with ISA Cybersecurity.

Wadeed is an incredibly passionate cybersecurity professional with more than 19 years experience in IT management, IT security management and IT enterprise architecture. Throughout his career he has implemented large information security programs and practices, and is highly effective at risk and operational management. Wadeed is successful at making critical decisions to protect the availability, integrity, and confidentiality of critical business and information systems. As much as Wadeed is recognized for his technical experience and knowledge, he is the epitome of a people leader who is always there for his team in his spare time.

He loves spending time with his family, eating Chinese cuisine with his friends and taking on the video gaming world. Today, Wadeed shares his insight and experience in incident preparedness planning.

Welcome Wadeed! Before we start, tell us a little about your role with ISA.

[00:01:50] **Wadeed Mian:** Sure. I'm currently the VP of digital forensics incident response. So basically anything within that umbrella falls under my work.

[00:01:57] **Tenielle Bogdan:** How long have you been in the industry? What's your experience with municipalities?

[00:02:02] **Wadeed Mian:** I've been in the tech industry for about 20 years. And our experience with municipalities varies from helping them stand up security solutions and architect them all the way through to incident response.

[00:02:16] **Tenielle Bogdan:** We've heard a lot about how the threat landscape is changing, not only for municipalities, but a lot of other organizations, with a big factor being the switch to a remote working environment. Why is the threat landscape increasing for municipalities outside of this?

[00:02:29] **Wadeed Mian:** You accurately said it – the landscape's evolving very rapidly and has been for a long time, but it has sort of accelerated in the past little bit amd the working from home has exacerbated it now. Where it has been particularly challenging for municipalities is a lot of threat actors have realized that municipalities are the gatekeepers for a lot of really, really sensitive information.There's corporate information and corporate espionage. Hacktivism comes in handy with that stuff, but if you're really talking about sensitive information in terms of records, municipalities are gold mines. Unfortunately there's a little bit of a reputation for municipalities. Their controls are not necessarily up to speed and they don't have the budgets of Fortune 500 companies.

So in terms of being able to invest the resources, the infrastructure, it tends to be a little bit behind targets.

[00:03:23] **Tenielle Bogdan:** I'm sure a key factor in that is preparation. How does preparation play a role in securing municipalities?

[00:03:30] **Wadeed Mian:** There's a variety of areas in particular, but by being able to build and develop a incident response plan and a detailed incident response plan that leverages your playbooks, you are in the best position to face a cyber breach or attack. You want to be able to build these, which obviously requires quite a bit of an investment, but you also need to keep them up to date and then you need to test them on a constant basis. Because what happens is as organizations evolve, inevitably people change and the roles change, and as they move on, people forget who was part of the incident response plan (IRP). So constantly testing and keeping your plans fresh help identify areas of improvement because as your infrastructure changes and evolves, so should your IRP.

[00:04:25] **Tenielle Bogdan:** I'm sure a key component in that is incident recognition as well, knowing when you've been attacked or when there's been a breach. Can you chat a little bit about that?

[00:04:32] **Wadeed Mian:** That's the critical part of an IRP. The first thing you want to do is understand who gets to make that call. What is the criteria? One of the things you don't want to do is be making ad hoc decisions under crisis.. You don't have the time to properly evaluate all the risks, the potential responses and all that kind of good stuff.

So the less decision-making that you do at that stage, the better. You want to build a criteria for yourself. You want to make sure the criteria covers what qualifies as a crisis, as a disaster, or as an incident, and how you categorize it. And based on the categorization, how do you invoke the right playbook? How do you involve the right people? I mean, it could be something as simple as paying a ransom. I'm just coming off a case where the customer lost 10 days worth of data. Their response to us was that significant data loss is a significant financial loss. We posed questions like “what is your criteria for paying the ransom and who gets to make that call?”, “do we need to engage your legal counsel?”, “do you have a breach coach that we should bring in?”. The more you these questions established, as well as a checklist for the situation, the better off you’re going to be. So, identifying a crisis becomes a lot more streamlined. It's not looking for an individual person to make an ad hoc decision on whether this is a disaster or not.

[00:06:12] **Tenielle Bogdan:** Who do you feel could be a good leader for cybersecurity within municipalities?

[00:06:24] **Wadeed Mian:** It really depends for municipalities, but we always recommend breach coaches. I can't recommend them enough. The main reason for that is these are professionals who've been through this experience. They know the threat landscape, they know the threat actors, they know the tactics, techniques, and procedures. There'll be able to guide you because a lot of times your response in terms of making a decision about the ransom, it really also depends on the threat. Are they the threat actors themselves? Are they the affiliates that are distributing? Are they the threatening type that are just sort of tossing the stuff around? How new is it? These are all parameters that need to be balanced.

I think there needs to be a decision-maker and that's typically, as I said, a breach coach, legal counsel, somewhere in there who makes the final decision, but it does need to be a collaborative effort in terms of providing them intelligence. You want to arm them with the information they need to make an educated decision.

Who is this particular ransomware developer? What's the impact? The other thing is it could be a very sophisticated ransomware, but fortunately it's been isolated to a relatively low impact area of the business or resources. You’re probably going to be a lot less in a lot less of a state of urgency to declare an emergency or pay the ransom if this is the case.

There's a lot of these parameters that need to be evaluated. And then once we armed the right people, then they can make an educated decision.

[00:08:00] **Tenielle Bogdan:** Elaborate a little more on a breach coach. Would that be someone internal to the municipality’s team or would that be through a third party?

[00:08:09] **Wadeed Mian:** I think all of the above, I think you'll find that it'll depend on the size of the municipality. You can spend all the money in the world and still not be a hundred percent secure. So there needs to be a balance between budget versus effective security – risk versus reward. I think some municipalities will want to have a full-time beach

coach on as their exposure is much higher. And then you'll have some of the smaller municipalities, for example, who may not be able to have someone full time. Now the options are to have a third-party that they subscribed to as needed, but there's also an option for municipalities to pool together for a single breach coach that services and a number of municipalities.

I think municipalities will have to evaluate risk versus reward in terms of how best to engage a breach coach.

[00:09:10] **Tenielle Bogdan:** When should a breach coach be involved? At what time should a breach coach be engaged with for municipalities?

[00:09:16] **Wadeed Mian:** As soon as possible. And I'm guessing you're you already knew that, but yes, as soon as possible. The reason being is a lot of folks who haven't experienced having been through a ransomware experience before have a tendency to panic and make knee-jerk reactions. These quick and irrational decisions can hurt your ability to recover quickly or to recover at all.

You want to engage your breach coach as soon as possible because they've been through it. They've seen it a dozen times. One of the first things that we do when we engage a customer is to calm them down. The first thing I say to them is, I know you're in every instinct, every fiber of your being is telling you to panic and, and, and hit every alarm and push buttons, but please do not. The best way to approach this is to take a step back, have a cool head and evaluate everything. You need to be able to evaluate who's doing what, what the best approach is and the plan, and validate the plan. Because if we just execute a plan, we may end up making things worse.

Typically the first attack, especially if it's a sophisticated attack, the first one is just the first step. There's a lot of stuff that happens after that and there's a lot of planning that has already happened before that. A breach coach brings this guidance to an organization that typically that hasn't been through this a number of times and helps them understand what's the best course of action.

It's actually, our CEO uses this example and I love it when you want to get somewhere that you've never been before, you want to bring someone who's been there. This is more true than true in digital forensics and incident response.

[00:11:51] **Tenielle Bogdan:** Can you elaborate further on communications in crisis and how that plays out within an IRP?

[00:12:13] **Wadeed Mian:** One of the first things we try and help customers with on the communication side is understanding that there's two directions for committee. There's the internal communication and then there's a communication externally. First and foremost, the knee-jerk reaction is to start sending out all these memos internally, which we stress that you cannot share too much information when an investigation is in progress. This is because you don’t know what kind of access the threat actors have. Again, a breach coach will be able to guide them through this.

You also want to be cognizant of what your communicating outside your organization because there is disclosure notification laws you might be under. Your legal counsel will tell you what you can and cannot share right away, because it may put some of your clients, customers, or patients at risk. It’s critical to understand what to communicate and when, and it's critical to have these two separate criteria is because what you're communicating internally and externally have different objectives.

[00:14:08] **Tenielle Bogdan:** We’ve chatted about the incident response plan and playbooks, but how are these decisions made and how are they developed?

[00:14:24] **Wadeed Mian:** The incident response plan and playbook work together. The incident response plan is the all encompassing, comprehensive approach, while the playbooks are the arms that work off it depending on the certain incident.

When I come into an organization and I have the opportunity to help them build both of these, because it really helps set the stage. This is where you're identifying who your incident team is, with representatives from each of the different departments. Then the IRP also takes into account specific structure in your organization.

Now the playbooks, and this is where it gets technical. And this is an area that I'm passionate about. They're far more specific to the threat itself. For example, we have a massive spike in demand right now for building ransomware-based playbooks for our customers. These playbooks drill down that the crisis is, what controls are currently in place and how do we leverage them? You'll want to look at your files and integrity monitoring solutions to see where your endpoints are and what controls you have on them, and whether there has been data exfiltration. The playbook will tell you exactly where to go. It's very specific and methodical.

[00:17:06] **Tenielle Bogdan:** Ransomware is something we're hearing more and more about. why are ransomware attacks increasing?

[00:17:13] **Wadeed Mian:** I'm being very candid, it's because they've been effective. A ton of statistics that'll show you just how much money is being paid out and just how prolific they are. Obviously with the bulk of the workforce now being remote has also expanded the footprint because you're no longer behind a corporate firewall and all those controls. A lot of organizations were forced into remote work and weren't equipped for it at the time. With less controls over BYOB devices and devices being accessed for a number of purposes, paired with the positive results that threat actors have been getting from ransomware, its becoming more and more common. I hate to put it this way, but for the threat actors, its not personal or emotional. It's purely business.

[00:19:56] **Tenielle Bogdan:** The biggest piece that we're finding through this is that the biggest threat is the lack of awareness in the simple solutions and things that can be done to safeguard municipalities and organizations. In your experience, what's one of the biggest gaps you see in customers or specifically municipality's plans when they're being executed?

[00:20:12] **Wadeed Mian:** As of late, one of the challenges we've been having is organizations either have an IRP that's very specific to this particular business as opposed to a comprehensive one. So when something happens outside of that business unit, there's a lot of confusion and delay. The reality is you want to minimize the time that you're able to invoke and execute. When there's a lot of time being spent on trying to figure out what are we going to do and who's responsible for this, the time spent on this is a big gap.

For example, centralized logging and retention is one of the things that really helps you track what a threat actor has been doing from a tactics and procedures from a basic perspective. Unfortunately, again, one of the circumstances where we've had is a client who did not have centralized logging, without which the threat actor was able to delete all the logs. In this circumstance, we had to "go in blind" without having that key information.

[00:21:55] **Tenielle Bogdan:** So centralized logs and backups are our two things to be aware of. But if you can provide our listeners with any other tactical piece of advice that they can take away and implement into their organizations tomorrow or next week, what would that be?

[00:22:09] **Wadeed Mian:** Definitely to engage an organization that does incident response. One of the key things also is you don't want to be negotiating contracts or trying to do the evaluation needed to contract a third-party in the event of an incident. You want to have affirmed that you've already got a relationship with and they know your environment so they are ready to go.

[00:22:34] **Tenielle Bogdan:** How can listeners get connected with you and ISA?

[00:22:37] **Wadeed Mian:** Listeners can always visit us at www.ISAcybersecurity.com or find us on LinkedIn for a lot of really informative blogs.

[00:22:46] **Tenielle Bogdan:** And make sure to check out our Municipal Cybersecurity Best Practices guidelines live on the technician website www.technationcanada.ca. A big thank you again to Wadeed and the entire team at ISA Cybersecurity. To get connected with them, head to their website, www.isacybersecurity.com or check out their amazing blog posts and articles on their LinkedIn page. Once again, thanks for tuning in.