Cyber Safe Cities Podcast

Dealing with Cyber Attacks with Sheldon Shaw, Former Vice President of Infrastructure and Innovation with Cyber New Brunswick

[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

Thanks for tuning in. I'm your host, Tenielle Bogdan, and today we are chatting with Sheldon Shaw, Vice-President of Innovation and Infrastructure with Cyber New Brunswick (CyberNB).

Shaw is a graduate of Acadia university in English and political science. Following graduation. He embarked on a career in national security spending time at two federal agencies focused on non-proliferation and cyberspace. Following this career in government, he went on to focus on cyber analytics, targeting the financial and industrial sectors.

Sheldon is currently the VP of Infrastructure and Innovation at CyberNB, where he continues to apply focus on critical infrastructure, operations, transparency, compliance, measures, and cyber analytics to combat cyber intrusions. We are very happy to have Sheldon on our podcast to share his experience in dealing with cyber attacks and steps to take when you've experienced one.

We are here with Sheldon Shaw, of CyberNB. Can you explain to us what your title is and what you do with the organization?

[00:01:36] **Sheldon:** I do have a title, although I never say it. So I get in trouble in meetings for not introducing myself as the vice president of innovation and infrastructure. Typically I just respond with I'm part of cyber MB and we work on critical infrastructure.

Some of the things that we're working on in cyber are really quite exciting. I think one of the key areas that we're working on is threat intelligence, so distributing threat intelligence out to our members that are in the critical infrastructure sector.

The other part that we're working on is analytics. So we are modeling attacks where you're building environments, allowing a attack to happen, and then taking the sensor data out of those environments and building analytics around them.

[00:02:34] **Tenielle:** That's awesome. How does the work you are doing in infrastructure apply to municipalities?

[00:02:40] **Sheldon:** We're pretty heavily involved in working on risk scenarios with municipalities, small and large I would say across the board municipalities have been underfunded to look at risk and they have a lot of infrastructure that they're managing and trying to move forward and operationalize.

Water services are a perfect example because I think going back 15 years ago, there was an attack on a dam and somebody forced the dam open and the water came out. So it's always been on our radar. We haven't seen too many attacks related to it in Canada, but I'm sure we will.

And that's something that is quite current with municipalities is the management of water. There's very few infrastructure within municipalities that use IOT, like roads, so there's really not a kind of electronic attack kind of surface for many of these areas.

I think the biggest thing we're seeing out there is municipalities really want to get a better handle on what is risk and how can they manage it.. There's lots of tools, lots of techniques that you can use. But I think we're there to help the municipalities work their way through all of the options..

[00:04:00] **Tenielle:** Some of the hot keywords currently are risk management and risk mitigation. In your opinion, do you think it's management or mitigation or both?

[00:04:11] **Sheldon:** I think you have to start with management before you get to the mitigation.

There's some blind spots, and we don't know, we can't secure. If you don't understand what assets you have, then you can't understand the accurate risk picture. There are some cool techniques now, so you can do including passive or active scans of your environment to find out what all your assets are, then kind of bring in all the vulnerabilities and put that into a database. Then you can look at it and ask what are the attacks that are happening? What are my risks right now?

One of the big things that I like to talk about is you could be the CAO of a municipality, but you're not the only one that should be managing the risk. I think risk starts with every single employee and their education and understanding of your assets and then policy frameworks, as well as who is accountable for it.

When should you be talking about risk? It's not something that you talk about once a year. It should be something you talk about almost every meeting or, or every week, and everybody should understand what their role is in risk management. Whether it comes to full time staff or summer students, everyone needs to be aware of risk.

Municipalities are heavy users of summer students who come in, get a laptop to work for a few months and they leave. Do you take the credentials off a laptop? Do you clean it and have the summer students going through training for these informational risks? If you haven't done that, that increases your risk.

[00:07:37] **Tenielle:** There's cyber attacks, and there's a security breaches. Chat about difference between those two.

[00:08:06] **Sheldon:** You know, a security breach, basically for me, is when you've been compromised. In a security attack, you may not have been compromised – you may have just seen the precursor of an attack. But both can be detrimental.

I think the first thing that that should happen in any event is knowing what is your PR strategy. How are you going to communicate the details of what just happened?

Ensure you're saying it in plain language, and you don't have to be very technical about it. I think the best way to describe an attack or a breach is just to speak in clear language about what happened, about what you know about the attack (the dates and times), who's working on it now, and whether or not personal or stakeholder information has been leaked or compromised. I think if you don't know the answer to these questions, its also okay to state that and be honest.

[00:09:45] **Tenielle:** In a perfect world, when a municipality experiences a breach or an attack they would simply consult their IRP and playbook and execute the plan. We know that not many municipalities have developed these pieces, so what is the first thing that they should do or consider when they've experienced a cyber event?

[00:10:04] **Sheldon:** If a municipality does not have a playbook or plan, they should look to do.

Playbooks are definitely a must-have. Another way of speaking about it as BCP, or business continuity planning. So if we are a compromised you know, what is our backup strategy? Do we have an offsite backup strategy? What is our cloud strategy?

The security policy is quite key for the topic that municipalities should keep top of mind. A lot of the municipalities that I've talked to have one, but it hasn't been updated in a while. They don't want to spend the money to do it, but I think a lot of this policy, you can borrow from others and ask other municipalities, to see how it can fit within your organization.

[00:11:56] **Tenielle:** What is a recommended timeframe for municipalities to look at and re-evaluate their security policies?

[00:12:05] **Sheldon:** It could be really dependent on the size of the municipality, but I think it’s good to look at them on a two year cycle. Larger municipalities may want to look at it every year. That could have a policy planning weekend or day where they go through and everybody makes sure that they're confident and that the policies are covering the situations that are, that are facing them.

[00:13:14] **Tenielle:** Let's chat about risk reviews. This is an area that you have much experience and expertise in.

[00:13:21] **Sheldon:** Understanding what assets you have is probably the key when you're doing a risk review.

We work with a variety of companies that are able to provide you a holistic view of your risk, which you should probably be reviewing on a monthly or weekly basis.

A matter of good executive management is to be able to talk about risk and evaluate your assets in terms of whether they are either decaying, are out of service, or are running older versions of software, and which ones need to be updated.

Those are all risk decisions and there's always a financial. There may be a big financial impact for you to modernize your infrastructure. But I wouldn't say there's a much larger impact on a larger financial consequences if you don't. We're seeing a lot of malware and crypto locker, you know, incidents based on older versions of software.

Certainly we, when I go meet with municipalities, we are recommending that they reach out to professionals in the industry. Most of the municipalities we work with have a managed security provider. We tend to touch base with those security providers and let them know that we're going to have a risk conversation. We like to work with these providers to evaluate the service that the municipality is receiving and where their risk might be or what gaps need to be filled.

And we make recommendations. We have many members of CyberNB that are companies that we recommend municipalities reach out to. and be that we can make recommendations to our municipalities and say, you should reach out to them.

[00:16:25] **Tenielle:** Can you speak anecdotally about a municipality responded really well to an incident or alternatively, some common errors that you see municipalities make in dealing with cyber attacks?

[00:16:38] **Sheldon:** One municipality in particular had a very strong understanding of their assets, which was shocking because there were a municipality that used a managed service provider. Although this piece of their municipality was outsources, their internal team had a very strong understanding of what their assets were, to the point of having detailed spreadsheets on them. They actually had evidence to show even though they were not a victim of an attack. But they had all of their ducks in a row, so to speak, and that was very promising. We were able to point them to some other provincial and federal policy instruments that they may have wanted to inherit, which they were open to.

I think one of the best things, and one of the best outcomes of our conversation was this idea of a virtual CIO, or Chief Information Security Officer. The idea of the virtual CISO is having someone on a contract basis, so not full-time, that a municipality could have for three to five hours a week where the person would be your virtual security officer. They would come in and do these sorts of things and walk them through either a tabletop exercise or an analytics exercise.

This municipality was very open to external advice, and I think that was really the key. What we see often is very insular activities where people start to see that maybe they need to only keep this in-house and they don't share as much intelligence about the attacks they’ve faced.They don't do a press release for two to three days, or they kept it hidden from their constituents. Those sorts of activities never move the ecosystem, and for many, can be very detrimental. And it usually leaks out and it's usually a really bad situation. So if you're attacked, you know, you should have a plan in place.

If the municipality I am referencing every does get attacked, they have all of the procedures in place to handle it.

[00:19:03] **Tenielle:** If a municipality is looking to learn more about the virtual CISO model, where should they look?

[00:19:22] **Sheldon:** They could reach out to reach out to us at CyberNB. And we could connect them to a few people in our membership ecosystem.

You can also Google the term and you can get access to some pretty good top talent. We also have a lot of top talent in the Maritimes as well. There's a lot of managed security providers that are part of our ecosystem that have really good talent that with whom I spent a lot of time in partnership conversations.

[00:21:18] **Tenielle:** When a municipality experiences and an attack or a breach, who is that first partner or external player they should look to engage with?

[00:21:31] **Sheldon:** If they've outsourced some of their IT, they should star with their managed security provider. They can assist in securing the data and then deciding who is going to do the heavy lifting, based on the contract they have.

There should be a checklist for every municipality with clear dialogue with every possible situation. What if they lose access to their email? Get on their cell phone and be able to do this or use a different device. You have to be prepared for that and a variety of other situations

If you're not well equipped, then you have to bring in somebody else. You'll need to hire specialists to come in and help out and secure everything and make sure that it hasn't gone any deeper in the network.

Your communications team should also be every meeting so there should be no surprises to them. You have to get them involved right in the beginning, so they can hear what is going on, which allows them to draft your messaging quickly. Once the messaging is drafted, this should be shared with your executive management team so there are no discrepancies. Different and inconsistent messaging causes a lot of confusion.

[00:23:29] **Tenielle:** Have you come across any resources that municipalities could have a look at regarding a cyber attack/breach checklist? Is there any documents that are already created that they could repurpose?

[00:23:39] **Sheldon:** When we do an engagement with the municipality, we have a what's called a municipality toolkit.

You can Google a lot of terms as well, as there are many resources that are free.

And then there are ones that can be built specifically for you, because I think there's quite a difference between a very small municipality and a very large municipality, which will cause your checklist to be quite different.

[00:24:42] **Tenielle:** So, if you could leave our listeners with one piece of information that you hope they remember, what would that be?

[00:24:51] **Sheldon:** Look into your municipalities checklist. These checklists are not one-size fits all, but it'll help us uncover all of the questions we don't have answers to

You don't need to feel burdened by the entire checklist at once, but start small. Maybe you only have three items currently like, who should we call? What are the phone numbers? Who is our contact with our managing service provider? Do we have 24/7 coverage with our managing service provider?. Some municipalities may not have that information at their fingertips.

Start with that little checklist process, which may start to elicit more questions and more concerns. I would go to your next meeting and ask for that checklist and then start creating it if you don't have it.

[00:26:02] **Tenielle:** Yeah, that's awesome. And look at what resources already out there too. There's resources through CyberNB as well as our Municipal Cybersecurity Best Practices guidelines. And again, reach out to other municipalities and see, see what you can learn from each other.

[00:26:20] **Sheldon:** Very well said

[00:26:25] **Tenielle:** a big thank you again to Sheldon Shaw for sharing his knowledge on cyber security for municipalities. To get connected with CyberNB, head to their website, cybernb.ca.