Cyber Safe Cities Podcast

Threat Vulnerability and Risk Assessment with Ashley Lukeeram, Global VP, ISC/OT Security with Tenable

[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 Ashley Lukeeram, Global VP with Tenable.

Ashley is accountable for Tenable's overall business strategy in Canada and leads a team of cybersecurity experts who help organizations address cybersecurity and risk management through Tenable's solutions and services. Ashley has over 20 years of experience in the IT industry. Starting his career in a consulting role on IT, infrastructure and security for enterprise customers, his passion for cybersecurity led him to managing the security program for Symantec and Microsoft distributors for the Africa region. He continued on his cybersecurity journey at industry leading companies, such as Rogers, Symantec, and RX. Prior to his tenure at Tenable, along with a master's degree in information technology from Cranfield university UK, Ashley also holds several industry certifications.

Ashley has been part of the industry advisory board of reboots privacy and security conference, and is currently an active member of TECHNATION and the cybersecurity threat exchange. Today, we are chatting with Ashley about threat vulnerability and risk assessments.

Welcome back everyone. We are so excited to have Ashley Lukeeram here today with us from Tenable. Tell us a little bit about your work at Tenable.

[00:02:12] **Ashley Lukeeram:** Absolutely. So like you mentioned, I'm the country leader for Tenable.So basically I work with folks across the country. Our responsibility is to work with a number of customers across different verticals in Canada, to help them address cyber security or we come in from an advisory point of view to give them the guidance needed and the type of solutions that can help them reduce risks throughout their environments.

[00:02:41] **Tenielle Bogdan:** How has tenable been involved with cybersecurity and municipalities specifically?

[00:02:46] **Ashley Lukeeram:** Terrible as a company has been investing significantly in Canada over the three and a half years. Some of the work that we've been doing is actually for organizations like TECHNATION, Public Safety Canada, and Canadian Cyber Threat Exchange. Through these different organizations, we have been providing different thought leadership to municipalities. Last year, I was personally involved with TECHNATION on drafting the Municipal Cybersecurity Best Practices.

Aside from these key things I just mentioned, we also on a day-to-day basis are interacting with different municipalities across the county. Very often again, the main reason clients come to Tenable is to understand where to start with their cybersecurity needs. Very often, it's a buzzword and people get confused. People have very few resources, so they come to us to have more of that cybersecurity program conversation. And therefore that's where we get involved.

[00:04:05] **Tenielle Bogdan:** So we've learnt over the past two years with COVID really shifted the working environment to remote and hybrid work, with a lot of vulnerabilities coming in.

Have you seen any other reasons for increased risk for municipalities?

[00:04:23] **Ashley Lukeeram:** The key word here is risk. So when we talk about. I think about it from two major angles. The first thing which we saw happening was that the municipalities had to increase their pace of digital transformation. As Canadian citizens, we have been looking at our means to provide more and more of these services online. We're starting to embrace more web applications again, with the goal of making those services easily accessible and as fast as possible to citizens.

The questions being asked are around where to star. Do we leverage infrastructures in the cloud? We've seen quite a bit of adoption from different cloud service providers, whether it's AWS, Google, Microsoft, and becoming more and more prevalent to municipalities.

As that pace of transformation has evolved a little bit faster, unfortunately so has the attack footprint for those municipalities. This is paired with an equally stressed timeframe with the pandemic. The amount of workload has increased with an expanded footprint, and many haven't necessarily increased their protection of the environment.

[00:08:01] **Tenielle Bogdan:** In chatting about the change of networks for remote employees, can you provide any guidance for municipalities that could help mitigate the risk that comes along specifically with the change in networks?

[00:08:13] **Ashley Lukeeram:** There are a number of things that could be done, but very important to start off with identity authentication. As you log into your devices, make sure you have either a strong password or multifactor authentication. There's a bunch of capabilities which municipalities are deploying out today.

Secondly, get back to the basics and take security awareness training. The foundational stuff is great to review and beware of, like how to detect a phishing attack and how to report it. A great practice is implementing this type of training for your entire staff so they know what not to click.

[00:09:20] **Tenielle Bogdan:** What are the motives of these threat actors that implement cyber attacks? Why are they targeting municipalities more?

[00:09:35] **Ashley Lukeeram:** When we look at municipalities, they're dealing with citizens like you and I, and very often, we're logging in to get different tablets and devices. Basically that means there is a lot of personal identifiable information (PII) within the environment that municipalities have in place today.

From a hacker point of view, this this is great. Data is king in this world. f they can get access to your personal information, they are all a lot of takers of that information for the right dollars. There is a black economy out there to actually leverage your identity information. These actors are looking to figure out how to access that data and turn it into cash.

The second area is what happens when an attack hits an organization. It's also a question of understanding how much of an impact that is going to create. In the case of a breach to a municipality, this also impacts the brand, and could have a political angle. The bottom line is that if a municipalities is breached, there is going to be a conversation around ransomware and what that payment will look like.

Another area is the defense around municipalities. There is a shortage in the cybersecurity workforce, which means less skilled people to work in this area and protect organizations. The hackers are aware of this and these environment are getting stretched more. With less people working in this area, all the hackers need is one, single loophole to get into these environments.

Lastly is the area of industrial control systems, which we also call operational techniques. If you think about IT systems, you're thinking about the treatments within municipalities. What we are seeing over the last couple of years is a convergence between traditional IT and OT/ISC infrastructure. These can be involving potential life or death situations. For example, if someone gets into a water treatment plant and makes a slight tweak on the amount of chlorine or any other chemicals going into the water, that's a big issue for people. By accessing these operational things within municipalities, it has very, very serious implication to citizens.

And therefore, it does make it a very attractive target for those bad people, bad people out there. They are targeted attacks. They are all very well known targets and the bad people know that they can get potential ransom out of those attacks.

[00:14:11] **Tenielle Bogdan:** Would you say that those targeted attackes are still crimes of opportunity?

[00:14:27] **Ashley Lukeeram:** Definitely the harder municipality or any organization can make it for the hacker, the less likely they are to experience a breach or attack. Just having one level of security is not enough. Just having antivirus softwar or a firewall is just not enough. I think it comes back to what's the size of the organization. What are the potential areas that are weak? Like any good hacker, the first thing they're going to do is a reconnaissance. They're going to come in, scan the environment and the network, just to understand what is your mechanism of defense.

[00:15:30] **Tenielle Bogdan:** And I'm sure that's why it's very important to know and keep track of what those potential vulnerabilities might be.

[00:15:37] **Ashley Lukeeram:** Absolutely. And more importantly, it has to be as close to real time as possible. You cannot survive in this world by doing an assessment twice per year and think you've done your due diligence. Cybersecurity is moving very fast, and we need have closer to real-time vulnerability assessments on the environment.

[00:16:03] **Tenielle Bogdan:** For a smaller municipality who might not have the vast cyber or IT team at their ready to deal with this constant re-evaluation, whose responsibility should that be?

[00:16:18] **Ashley Lukeeram:** This is where it becomes a conversation about who owns risk. Who owns cyber risk in the traditional days was a cybersecurity group. As citizens and folks within municipalities, we need to make sure that everyone in the organization understands cyber and cyber risk. We need to start bringing in risk culture to organizations. This can be done with basic training and making sure your staff understands that they can actually greatly impact the entire municipality.

I would say the number of things that can be done in terms of assessments, don't necessarily need to have all the bells and whistles in terms of technology from day one, but you could start with very simple assessment of your processes and operational workflows. You can start tweaking some of your business processes to help minimize your risk.

[00:17:46] **Tenielle Bogdan:** You touched a little right there on risk assessments. What are some other risk assessments that municipalities can undergo?

[00:17:52] **Ashley Lukeeram:** What I just touched on what more of a qualitative risk assessment. We could also come in and do a questionnaire, addressing things like how are you doing backup? What type of controls you have in place? You could also ask these same questions to your suppliers. Municipalities, like many other organizations have third parties coming in to provide different services. When these organization are coming in, it would be a good thing just to have a checklist of controls that you would like to see from those third parties before they provide you the service.

The second area here is really getting into the quantitative measurement of your risk. To do this properly, It's very important for municipalities to put a vulnerability management program in place. This is where you would need to look at capabilities from the industry to basically come and scan your entire footprint: your traditional servers, your endpoints, your cloud, your remote workforce infrastructure, and give you a sense of which job vulnerabilities exist in your environment. At the same time, this give you a better understanding of which type of assets that you have in your organization. If you cannot see what you have, you won't be able to protect yourself. This is also why your asset and risk reviews need to be on a continuous basis.

Many organizations that we've dealt with in the past and still today, have a contractor coming in to do a pen testing once per year or twice a week. Yes, this is a start but this is not enough. The question that comes to the table very often is this, what are the new vulnerabilities out today? Typically, the business is going to come and ask the question of how secure are we against this new vulnerability?

What we see often is organizations pull out their last report from six months ago, which will not contain the answer because this is a new vulnerability and threat. So the point is that you need to continually evolve. You have to get to that point where you understand that risk is not static. It changes every day, every minute. And so all the threat actors and bad actors our there. we need to look at our assets, the front intelligence, and then the potential impact as often as we can.

[00:21:21] **Tenielle Bogdan:** That's great. I really like your point about the vulnerability management plan. Can you chat with us about how that feeds into an emergency preparedness plan or emergency response plan (ERP)?

[00:21:34] **Ashley Lukeeram:** I would say a vulnerability management plan is a foundational component of a cyber security program. When you look at IT and emergency response plans, this is your guide to how your organization need to react. When we talk about vulnerability management plans, what we're talking about is being as proactive as possible, trying to reduce the likelihood of those situations and breaches. So the more you know about your vulnerabilities, hopefully you're going to have more time to work with your IT to go and patch and remediate and potential risks, as well as reduce the number of emergency responses that you're going to have to make. By no means, are you going to have zero incidents, but by being proactive, we can hopefully reduce the likelihood.

[00:22:37] **Tenielle Bogdan:** What is a success story that you can share from an organization that either you have dealt with or that you've known about who has eliminated the potential for a cyber attack or breach through proper preparedness?

[00:22:50] **Ashley Lukeeram:** The one that I can think of is actually a municipality Western Canada. This goes back to end of 2019. The municipality was quite small with only two resources for the cybersecurity program, with a total staff of around 2,500 employees. At the time, they came to us for a conversation around their struggles as a business with limited resources. With this, they were only able to get visibility of what was out there in their environment but unable to go in and scan further because as they scanned further, they were finding more and more vulnerabilities. With all of these increasing vulnerabilities, the municipality was in a reactive scenario.

What they decided to pursue was penetration testing on their system to help diagnose some of the gaps. This is a risk-based vulnerability management set of requirements. By bringing us in to help assess this, their team of two full-time employees was able to gain a greater sense of how to secure their man vulnerabilities with not increasing their number of staff.

What they also did is better prioritization of which vulnerability to fix first. Yes, they are still finding a lot, but through capabilities that's out there today, we have enough intelligence to advise them which one to tackle first. At the same time, this organization is starting to think about how to expand their coverage into their industrial control systems, which we are currently looking at for them.

[00:25:58] **Tenielle Bogdan:** And would you say that with kind of the expanded training and awareness within this particular organization that there was a shift in the culture around cybersecurity?

[00:26:08] **Ashley Lukeeram:** Yes. Definitely more awareness that it's an ongoing risk for them. If we go back to 2019, they were doing just an assessment what they were aware of. Now, the fact that they have some automation that's helping them, there is definitely more of an appetite to go and discover as much as possible.

[00:26:46] **Tenielle Bogdan:** If you can provide our listeners one tactical piece of advice to remember from our conversation today, what would that be?

[00:26:58] **Ashley Lukeeram:** Cyber hygiene is extremely important. This world of cybersecurity has a lot of possibilities out there. There's a lot of buzzwords, but truly when we talk about stick to the basics, really know your assets and know your vulnerabilities. From there, you can figure out where to go and what protection mechanisms to put in place. Its as if you're moving into a brand new house, and now you need to think about where to put physical security cameras. You'll first start with identifying all the points of entry – windows, doors, basement access, etc.. The same is how we should approach cybersecurity. Don't' try to boil the ocean – stick to the basics.

[00:27:52] **Tenielle Bogdan:** A big thank you again to Ashley and his team at Tenable for taking the time to chat with us today. To get connected with Tenable or to learn more about their services, head to their website at www.tenable.com. As always. If you are interested in learning more about how to enhance your organization's cybersecurity head to technationcanada.ca and check out our Municipal Cybersecurity Best Practices Guidelines. Thanks for tuning in and stay cyber safe.