Cyber Safe Cities Podcast

Managing Third-Party Vendors and Risk with Tyson Johnson, Former CEO of CyberNB

Tenielle

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 I'll be speaking with Tyson Johnson, CEO of Cyber New Brunswick (CyberNB). Tyson has worked in both the public and private sectors over the course of his career. Starting in the federal civil service, Tyson developed hands-on experience across the entire spectrum of issues facing canvas foreign and domestic threats. After departing the government of Canada, Tyson spent the next number of years building and supporting enterprise risk management platforms for multi-national organizations in both financial services and electronics manufacturing. It was during this period that Tyson obtained his master's designation from the Fletcher School of International Law and Diplomacy at Tufts University.

Prior to his tenure with CyberNB, Tyson led BrightPlanet, a US-based big data pioneer as its vice president of business development and strategy. In this role, Tyson helped shape BrightPlanet into a successful member of the data and analytics ecosystem to support risk management across government and industry. This included a key focus on threat identification and cybersecurity initiatives.

Today, Tyson leads CyberNB as it coordinates government industry and academia to support cybersecurity in critical infrastructure protection across Canada. We are excited to have Tyson on today to talk about third-party arrangements and how they can affect your organization's cyber hygiene.

Alrighty, hello everyone! I'm very, very happy to have with me here Tyson Johnson, chief executive officer with Cyber NB. How's it going? How's your day?

Tyson

So far, so good. It's a great day here and we're excited for the weeks and months ahead as we get ready to move into our new cyber center down the street. So lots of exciting things happening here at CyberNB.

Tenielle

Right on. Where are you based out of?

Tyson

We're in Fredericton, New Brunswick in the East Coast and then working with partners across Canada.

Tenielle

Fantastic, awesome. So, Tyson, chat a little bit about your experience in cybersecurity, your work with CyberNB, and how long you've been there?

Tyson

So I've been with CyberNB a little over four years now, but my background in all things enterprise risk, security and cyber stems back my entire career.

I exited out of university and went into the intelligence service here in Canada, where I had a great introduction into all aspects of threat, including the digital cyber threat risk exposures. Worked in big industry; I went into banking then into electronics manufacturing, outsourced electronics manufacturing in a global footprint and worked closely with the enterprise risk partners in those large entities. Learned a lot along the way around all aspects of risk management from a pure security side to how you mitigate it through contractual exposure and review and in insurance. Then I went to work for a big data firm that collected open-sourced unstructured information to support advanced analytics for threat detection that supported a lot of organizations and government agencies. And then I received the tap on the shoulder to come out and help move CyberNB forward.

So for the last—let's say four plus years—I've been here with CyberNB in our critical infrastructure protection network, and we're excited about where we've come from and certainly where we're heading.

Tenielle

That's awesome. CyberNB obviously has extensive experience in working with municipalities. Chat a little bit about your experience and any shifts, I guess you've seen within the past kind of three to five years since you started with the company to where we are now.

Tyson

Great question. I think the biggest change we've seen—that continues, it's not going away—is just the ever-increasing threat landscape that organizations, in general, and certainly municipalities start to face. What that means is almost everything is now connected to the internet unlike years ago, where in each year it seems to double or triple or, exponentially grow in terms of the number of connected devices. And we're certainly connecting devices for all the right reasons. We want to have more data, more insights on how to better manage in the case of municipalities; how to better understand usage by citizens; how to better manage things like water and waste; and how to you better manage all the different municipal deliveries (i.e., the services that you deliver to your citizens).

But with that, you're now introducing new threat into the landscape. So, you're literally increasing that digital footprint that you have as a municipality.

And so that's the biggest trend we've seen is—that what might've been 10 years ago as simple as saying, 'well, the only thing that's connected is our IT System and it's simply the software that we're receiving emails from vendors or internally we use it systems to track certain metrics'—now you have IOT devices connected; you have machinery that's operating your roads and different technologies all around your municipality that are talking to each other and all that data is being saved somewhere; and then you want to have different people access that data. So, your threat landscape, your digital threat landscape—your digital world if you will—has grown exponentially.

And that's the biggest change that we're seeing—or the continuous trend we're seeing—is that if you didn't have your arms around cyber risk or digital resiliency back when things were simple, then you're going to struggle today because you likely don't even understand the size of your risk footprint or your digital footprint in today's new world.

So those are the big things that we see municipalities are really struggling to understand and get their arms around.

Tenielle

Yeah, absolutely. And I completely agree with the connectivity and I think the connectivity plays right into what we're chatting about today. In third-parties and dealing with your third-party vendors obviously you can go super, super in-depth to what risk management looks like with those third-party vendors. But keeping in mind that municipalities are small organizations. They don't have big, big IT teams or chief IT officers for a lot of them.

So, let's touch a little bit on the base level of what are some of the questions that you need to be asking those third-party vendors on a really, really basic level.

Tyson

Absolutely, and I think you're right on to say, "how do we make this?"

These are business questions that we need to be asking. So the same way that you might ask questions on, are you financially solvent? Are you able to execute on the contract while on the cybersecurity side?

Questions like: Does your company/organization have a cybersecurity certification for your business? Are you CyberSecure Canada certified? Are you CMMC certified out of the states? Are you ISO certified? What business certification do you have that could demonstrate you have hygiene in place that I can trust or that I can hold up to the light of day? That would be one question.

Another question would be: Do you have employee awareness programs in place for cybersecurity? Human factors still remain the largest risk in the cyberspace. So, what proof do you have that the employees—who in most organizations take things like, workplace safety training and WHMIS training—are trained. Well, there's now cybersecurity training and digital hygiene training that your staff need to have. So asking your vendors, can you demonstrate what your awareness program is for cyber.

Another question: Do you keep all of your technology software, et cetera, up to date and patched? Real simple question. They should be able to provide you with an answer, if they can't, that should be a red flag to you.

Do you have a CIO (chief IT officer), a CSO (chief security officer), an IT director? Do you have somebody who's functionally in charge of making sure that there's digital resiliency in cyber hygiene in your organization? If they come back with a no, or can't answer again, another red flag.

And has a vendor recently had a penetration test conducted on its infrastructure on its business systems. Again, if the answer is no, that's a red flag, because these are all best practices.

If they're selling you a product; if you're buying something for your water systems, et cetera; is there a certification on that product, a digital certification that is common criteria certified? What might it be? Do you have something?

We could often make the parallel to the building a house or buying a toaster: If it's not ULC stamped or CSA stamped, you would never install it in your house, you would never plug it into your wall. If it was a light fixture, you would never trust it to not burn your house down. We're working closely with a number of global standards groups and what we need to do is get to a place where global standards—or best practice standards—can be asked for and demanded by companies; and so, that's another key question to ask.

Do you have a privacy certification? How do you protect data? You may have the greatest product security, cybersecurity in place for your products; you may do penetration tests on your infrastructure and you may have cyber awareness programs but if you're not protecting my data correctly—that can be stolen, or taken, or leaked—then I'm just as exposed.

So those are the key questions I would say. They're simple, they're easy to add and they demand an answer; and every organization going forward should be demanding these answers.

Tenielle

Awesome. And those are questions, I guess, that you could be asking at any point throughout the relationship, but I'm sure are equally as important when you're going out and procuring those vendors, correct?

Tyson

Certainly, when you're on the front-end of trying to find a new vendor for something and then of course with your current vendors; you should be demonstrating your roadmap. So, maybe day one, I'm saying, we're working towards certification, but we're just not quite there yet. Okay. As long as you're showing me that you're making progress. So then if we're coming for contract renewal or I'm checking in on you, show me how you're hitting your milestones, show me how you're advancing your cybersecurity readiness posture as an organization. Those milestones should be connected to your contract, they should be connected to performance and SLA is within your contracts. It all starts to connect and it all makes sense. We do it already on the physical side, and already on the financial side; this is just another dimension of risk that companies/organizations and municipalities need to add to the risk dimensions.

That's why this isn't something difficult or only people you should know. This is business. This is business speak, and this is just good business.

Tenielle

Yeah, that's awesome.

So, rewinding all the way back to chat about the types of assets that could be vulnerable with your third-party vendors. Let's dive into a little bit on that front.

Obviously, we can talk about information, we can talk about everything that you provide them and how that could actually impact your municipality.

Tyson

Yeah, it's an interesting kind of multidimensional chess going on here. So, I think on one dimension, it's pretty simple to think through and say, “okay, if I did a contract mapping exercise of my municipality,” I say, “well, who do we have contracts with?””

You would find you have managed services providers in the IT and cybersecurity space; you have software vendors and hardware vendors; potentially IT, IOT or OT device companies that you work with that you’ve subcontracted; you probably have a third-party legal firm that you work with; you probably have contractors for service and support, whether it's for your roads, maintenance or water systems; you have third-party private security firms for the physical side of things.

Now, so you'd go ahead and map out all your contracts to say, “who do we have. Relationships with?” and you'd realize pretty quickly that you pretty much have a digital engagement in one way or another with all those groups. They're either sending you emails back and forth; they have access to some critical system that you need to run your municipality, et cetera.

So you would map them out and say, “which ones do I, or don't I have a digital relationship with? Of those I have a digital relationship with that habit some type of digital footprint inside my municipality, which ones are the most significant?” You'd then map those out.

The other one is to realize that sometimes it's two things. One is I could have very little digital footprint with you. We talked a little bit earlier about it prior to going on air here where, you think about WannaCry. When WannaCry took down Maersk, it was a contract accounting firm that sent an Excel file and that was the extent of that digital relationship between these two organizations. And so, you don't need a giant digital footprint if you're not leveraging, up-to-date patched software; if you're not having great, employee awareness programs implemented, then that compromised Excel file that gets in through your system can take you down just as easy as the company that manages your entire, water filtration system for the municipality that doesn't have good hygiene on its technology.

So looking at, do you have solid awareness, patch management, cyber hygiene, digital hygiene in place, and what's the size of that digital footprint you manage or operate on my behalf? Those would be the areas I would look at.

Tenielle

Yeah, that's awesome. And obviously employee awareness is the biggest piece—and I think that'll be fed through all of our conversations on this podcast—is making sure your staff is engaged and the onus doesn't fall on one person. There should be a definite leader and someone owning the pack, but that cybersecurity needs to be intertwined through all aspects of the business, as we found out.

So, I guess chatting about employee awareness, what are some things that your internal team can do to protect those external relationships a super base level?

We've talked about the questions, we've talked about anything else, but is there anything else that can be happening internally to protect what's happening with those external contractors?

Tyson

Yeah, it's fascinating topic and it, and again, we really empathize with the municipalities. Many of the Canada's municipalities are small, so if you have an internal team then things like planning the quarterly reviews of your key vendors for those that have the highest risk exposure into your organization. And again, this isn't IT, IOT or OT, this is business risk management.

This is the same as you asking a vendor that they could demonstrate that they're capable of delivering on time, and you'd want to stay on top of that. This is the same thing you want to stay on top of it. Can you show us that you've delivered employee awareness for this quarter within your organization? Can you show us that you have recently managed the patch that you've updated the patches for that software that you have installed in our systems? Can you demonstrate that you did actually do a pen test against your systems, as you said you would on an annual basis?

So that internal team needs to hold those external vendors and teams accountable and, and really becomes an auditing process. And I know people don't like the word audit, that doesn't have any sex appeal to it, but good hygiene requires ongoing overview to make sure that people/companies are doing what they say they're doing.

That would be the best advice, this proactive risk management approach that you do in all other aspects of your life into your cyber/digital hygiene practices. And just add it in as deliverables for your internal team to keep the finger on the pulse of these external vendors.

Tenielle

That's awesome. Let's chat a little bit about some of the incidents we've seen across Canadian municipalities in the last couple of years.

We know that that your firm has had a lot of experience with many of these municipalities. So, if you could pinpoint one and take some provide some lessons learned from those to our listeners, that would be fantastic.

Tyson

Yeah, the municipal incidents that have happened, some of them have been very public. I mean, Stratford hats off to Stratford who were hit pretty hard.

A few years back and they made a point of saying, 'we're going to come public here and we're going to be a poster child for how we didn't do it right and how we got it right; and what we stress now.' And so challenge was, lessons get learned, but sometimes not fast enough.

And so, City of St. John here in the East Coast was hit pretty hard because it was under-resourced and had the inability to ensure the right controls were in place. And again, cyber hygiene, digital hygiene across the third-party environment was not being given the level of importance that it needs.

We see this in other municipalities. Recently, there was another incident in another municipality where it was bad luck, but fortunately it's preventable. It's not necessarily luck, it's about not keeping the doors open when they need to be closed.

So, I think one of the biggest things we see in what we try/stress is you're not reinventing a wheel here. There are playbooks out there from other municipalities that have been hit that are prepared to share what they've learned, but you have to be interested in this; you have to take this seriously. Like the very first question we started with here, the threat landscape is getting larger, not smaller.

If ransomware becomes the new dialing for dollars, this is the new scheme that we used to get calls about some wealthy Saudi prince that wanted to exfiltrate money out (i.e. "Can you just give me your bank account?"). This is the new dialing for dollars, Ransomware is the new dialing for dollars simple fraud scheme that low-level organized crime/criminals are able to exercise because we don't have enough controls in place. And municipalities, unfortunately, are a soft underbelly for this because of all these reasons that we just talked about: they're understaffed, underfunded, too busy putting out fires and keeping their municipality and their operations happening; assuming hygiene is being done by third-party vendors; assuming they can trust parties that they're working with.

I think one of the biggest—and I'm glad we're not here, I'm glad we're not talking about this—frustrations or myths is that people will say things like, "we have cyber insurance or we'll just pay the ransom," that's not prevention. That's not stopping something from happening.

You're assuming that, on a bad day there's some easy button you're going to hit where the insurance company will pay a ransom and everything gets turned back on because the bad guys are really nice guys and it's a small blip on the screen and everyone goes back to work. That's not how this rolls, this is not how this ends and we're seeing this.

What we're seeing across municipalities with the incidents that we've supported/helped or had some type of insight is the prevention side; it's hard work, but it's much more valuable. And we're actually seeing—as we have a number of insurance partners—is the ability for people/municipalities/organizations in general to get reinsured policies renewed or get a policy in the first place is dwindling because the actuaries in these insurance firms say, "if I can't measure how much you're taking this seriously and reducing your exposures, I'm not underwriting you."

And so, the house of cards is falling in on municipalities that aren't being proactive and upfront on things like third-party vendor screening and management because there's no backend support anymore; there is no insurance anymore.

There is no support for you on the backend because if you're not doing the right thing on the frontend, the backend is walking away from you.

Tenielle

Right on and you touched about playbooks, so this is a good time to plug our Municipal Cybersecurity Best Practices guidelines that's up on the TECHNATION website and it's a great resource for municipalities to have a peek at on a baseline level. We've really tried to keep that document super on the ground level, very readable, very digestible on that front.

Chatting about municipalities: obviously time, resource and capital are big barriers when it comes to just overall cybersecurity wellness and "hygiene," as you said—I really like that word. What's one tactical thing—if a municipality has no experience in cybersecurity they've really kind of touched on this baseline—what's the first thing they should do in regards to their third-party vendors and the risks that come alongside?

Tyson

Great question. And I certainly agree with you. I think the work that a TECHNATION is doing to provide some of these insights for municipalities are the baseline standards. This has to become your starting point for everything.

But if there was one big takeaway that I think is digestible and something that all these municipalities do: if you're a municipality that does not have your own security operating center or IT support group, or if you're outsourcing to a third-party managed services provider, ensure that relationship is managed closely.

What is the service level agreement? What are you asking of them? What services are they providing to you to answer those questions that we talked about earlier, that they should be asking on your behalf? Can they look at your environment that they're monitoring on your behalf? And make sure that the right questions being asked.

Can you engage a virtual CSO? Can you do a contract CSO on a few hours a month or a few hours a week that can come in and ask those hard questions for you and take a look at things? That would be the step I think is critical.

If you're big enough as a municipality where you have your own IT group and you have your own operating center and you're monitoring your own environments, don't let that group run autonomously. Make sure as the CAO or the leadership team of that municipality, that you're asking the hard questions that you can learn from these documents that TECHNATION has published. Ask, "please explain to me how we're mitigating this. How are we mitigating that? What have you done on this?"

If it's not your managed services provider that you're putting the thumb on, it should be your internal IT cybersecurity team that you're putting the thumb on. Get engaged, get knowledgeable, ask hard questions and demand answers.

Tenielle

Right on, I think that's awesome.

Tyson

A couple of things we can do to help is:

We have a tactical light risk assessment that Shelton Shaw from our team leads with our innovation infrastructure team here at Cyber NB which helps municipalities, do a base level review of what are they doing right now and where do they need to dig deeper.

Another one would be the transparency center initiative that we're running.

We are looking at demanding that organizations show their business certification for cyber hygiene and their product certification for their devices that they're installing/selling into the marketplace. And then privacy certifications. How are

they protecting data and protecting the information that they're in charge of?

The other thing I would say that municipalities need to appreciate is that 'global standards' is a conversation that's happening everywhere. And if you're not engaged in paying attention to what's happening around you, it'll happen to you.

For those municipalities that want to make sure they're out on the frontend of this and that they have a voice in this conversation, they should get engaged. Like any good business continuity plan or any good risk management plan, somebody on their team should be responsibly charged with monitoring, understanding and paying attention to what's going on in the cybersecurity world. And if it's not someone on their staff, then on their managed services provider, let somebody have that role and report to them.

Those would be some other I think critical areas and steps that municipalities need to take into consideration and lean on the TECHNATIONs, lean on the Cyber NBs that have resources and insights that can help.

This is what we're here for, you (i.e. municipalities) are not alone. This is not foreign. This is business risk management in the digital world and we're here to help.

Tenielle

That concludes this episode of the cyber safe cities podcast.

A big thank you to Tyson Johnson from Cyber NB for taking the time to chat with us today and sharing his expertise in dealing with third-party vendors and the risks associated.

For more information on CyberNB or to get connected with their team, head to www.cybernb.ca or for more information on how your municipality can get started in enhancing your cyber hygiene, head to technationcanada.ca and check out our Municipal Cybersecurity Best Practices guidelines.