Cyber Safe Cities Podcast

General Incident Management with Randy Purse, Senior Cybersecurity Advisor with the Rogers Cybersecure Catalyst

[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 Dr. Randy Purse, Senior Cybersecurity advisor with the Rogers Cybersecure Catalyst. A veteran, Randy served in the Royal Canadian Navy for 26+ years, including a variety of security roles. He then moved into the public service at the communication security establishment, also known as the Canadian Center for Cybersecurity, where he led the development of IT and security training for the federal government followed by assuming the role as the strategic advisor for cybersecurity training. He was previously the Director of Cybersecurity Standards and the VP of Future Workforce Development at TECHNATION Canada.

At the catalyst, he focuses his efforts on designing and facilitating effective cybersecurity training and education for a variety of professional audiences. We are very excited to have Randy on our podcast today to chat about general incident management.

[00:01:29] **Tenielle Bogdan:** For those of our listeners who are unaware, can you tell us a little bit about the work that happens at the catalyst?

[00:01:37] **Randy Purse:** The catalyst is a cybersecurity center of excellence within Canada. It's very unique. We're housed within Ryerson university but a separate entity, and we're primarily there to support cybersecurity activities and initiatives in Canada.

We have a number of initiatives ongoing. There's the accelerated cybersecurity training program, which is basically taking people not necessarily any technical background and putting them through a seven month process, and graduating them into entry level positions. That's a real stellar program within the catalyst.

We have a cybersecurity accelerator basically trying to create and help early stage Canadian companies, cybersecurity companies grow international into national and international companies. We have the policy exchange, which is of interest to municipalities because we're dealing with the national, provincial and international policy issues within cybersecurity. And of course we do quite a bit of training. We have training in e-learning, which is again of interest to municipalities. We have a cyber range where people could get hands-on training in a virtualized setting, and it's available all across Canada.

So anybody who has an IT or cybersecurity team that wants hands-on skills based training, we can do that. We also have a number of training courses that we're working on. And finally there's is there's a cyber secure program that's applicable to primarily small, medium enterprises, but it is a e-learning program that basically runs through a number of different topic areas that are of interest to leaders and it professionals. And finally, we're working with the government of Ontario on putting together their program for the broader public sector.

So it's quite a bit for a very small team but we're really trying to move the yardsticks in the cybersecurity domain.

[00:03:42] Tenielle Bogdan: And for those of you that are unaware Randy is an alumni of TECHNATION, who was our VP of Future Workforce Development before his work with the Catalyst.

In your role with catalyst, you covered a vast range of projects. What would be the one you say that's taking up the most of your time or that is the most interesting?

[00:04:01] Randy Purse: Since I left TECHNATION, I'm focusing my energies on cybersecurity training and education for whether it be corporate public sector or other entities in the commercial sector, doing whatever's required in order to make sure that people get the training they need.

It's very key, particularly in cybersecurity, because I think there's this misperception around cybersecurity that it's a completely technical field and you need technical expertise to do it well.

That's not the case. Our training hits a number of strata within organizational cybersecurity, including leaders, employees, it professionals, cyber security professionals and anybody else, IT managers and anybody else who might need to know.

And I also continue to do some minor consulting on management and cybersecurity management.

[00:05:03] Tenielle Bogdan: You have a pretty extensive past with training as well. Chat with us a little bit about your experience and training in cybersecurity.

[00:05:12] Randy Purse: Well, like a lot of people in the security field, I've come from the military.

We get basically embedded into a security culture in those types of roles. And so, we learn an awful lot through both training and experience in our lives. I spent 27 years with the military, and in that time I had a variety of different security roles, including physical personal personnel and IT security protection.

My interest in IT started to grow later on in my career, as I started to move into training development within the Canadian Armed Forces. I started to see more requirements around IT training. In conjunction with that, I was involved in my operational life as an information system security officer, and I was also involved in information operation plans at the very start of the cyber challenges facing the world at that time.

When I moved over to training and development, I started to focus more on operational walls and IT. I got my master's in it in education and then I retired from the military and moved into the communication security establishment, where I was with the IT security learning center and primarily responsible for Federal IT security training. While there I also got my PhD and I became the strategic advisor for cybersecurity training education for the Canadian Center for Cybersecurity.

It was a great job, but I reached the pinnacle of what I considered to be that career. Then I said, okay, that's enough. I need to retire again. So I had a retirement from the military than a retirement from the public service, and that's when I joined TECHNATION. I was also working with the catalyst at the time on an occasional casual basis doing consulting, training and education activities.

I've had a, quite a life within the last couple of decades in cybersecurity. My time with TECHNATION was particularly rich because I was working on the AI and Cybersecurity Skills Initiative (AICSI) as well as the Municipal Cybersecurity Best Practices (MCBP) Initiative.

[00:07:51] Tenielle Bogdan: You've been in the cybersecurity realm and security realm for a long time. But today we're talking about incident management which I think is a perfect topic for, for us to pick your brain about and to, to learn about your experience. So incident management is huge. If you could flag one area that's the most important or that municipalities should be paying attention to what area would that be?

[00:08:13] Randy Purse: The one thing about incident management is as a topic, its quite large, and a bit broader than just security issues. Incident management and the sub subset of that, which is incident response, which points to something that should be in place regardless of the cyber threat.

I think as it pertains to cybersecurity specifically, There's lots of stress on having an incident management plan.

The incident management plan and an incident response plan, also known as an IRP, is very important.

In order for an incident response plan to actually properly work, you need proper governance and proper cybersecurity governance that will allow for effective and timely decision making the even of an incident. Decision-making goes beyond awareness of the mitigations of the incident and include anything to do with crisis management and communications resources allocation.

Allocation of people within your organization is key to any IRP. Where are you going to get expert resources? Who's going to make the decision to pay for those? How are you going to connect with the media? What kind of internal communications are you going to need? Who's going to be an authority on messaging during an incident?

All of these fall under general governance. They're included in the plan, but the plan is merely words on paper. How do those decisions get made during an incident? Who has the responsibilities and authorities throughout the organization is also very important.

[00:11:20] **Tenielle Bogdan:**. So in talking about governance and using a "top down" approach, ts there any interesting policies that you've come across that municipalities have implemented or anything on that governance level that has stuck out to you?

[00:11:43] **Randy Purse:** There's a lot of what, what the industry calls, GRC governance, risk and compliance advice out there.

I think one of the things that municipalities should keep in mind is the access they have toa variety of resources, especially when looking at their governance. When they're looking at things, what they should be doing is looking at how their incident response runs through what their processes are and then finding somebody who's in legal counsel, or some sort of breach coach to help them with the nuanced messaging, the nuance structures, the liabilities and legal issues and the compliance requirements so that they could kind of get a good idea.

From a legal perspective, take a look at your plan, take a look at your governance and make sure that you have these technical points and and what every potential challenge there might be with respect to your legal positioning. That's a fairly large risk within the municipal space because you're dealing with citizens.

You're dealing with corporate data. You may have other municipal businesses, et cetera, that you have information and data that, that you're responsible for. You have tax rules, you have a bunch of different things that you're responsible for, and you should be very clearly aware of the risks associated with it.

And if you're not certain on that and let's face it, most municipalities in Canada are maybe not certain about the risks. They should at least bring in someone to help them understand those risks and what the option options are around with handling and mitigate, mitigating any risks that are as a result of the cyber threat.

[00:13:52] **Tenielle Bogdan:** That's definitely a common thread that we're seeing through a lot of these conversations in finding those external partners and finding those folks that excel in areas that municipalities naturally aren't meant to excel in.

[00:14:18] **Randy Purse:** The largest percentage of our corporate entities in Canada are small, medium enterprises. In fact, most of them have less than a hundred employees. There are over 4,000 municipalities in Canada, but there are not many large ones. Most municipalities in Canada are very small, and they might have a Mayor, town manager, CAO, or another sort of chief administrator. They probably don't have the expertise in-house to help them with their cyber needs.

One thing that municipalities may not be aware of is that you don't need to spend a lot of money on getting the right help. This could be coming to you inexpensively, and there's a lot of increasingly articulate legal minds working in the cybersecurity space in Canada. And there's a lot of good advice online within these firms.

[00:15:48] **Tenielle Bogdan:** What's something you think would surprise our listeners about incident management, something that's new or cutting edge, or just that flies under the radar?

[00:15:59] **Randy Purse:** I think the thing that most municipalities, struggle with, is that when the hear the word "cyber", they assume it is only an IT problem.

Cybersecurity is an organizational problem, so you need your whole organization involved to approach it effectively.I think that that's the message that if there's one message that I wanted to get through, that's cybersecurity is not just a technical problem.

Sure. There's technical elements to it, especially in the digital workplace and the digital world. But generally when we point to things like planning and governance, both of those are non-technical, and they can both be done with very little technical knowledge.

[00:17:50] **Tenielle Bogdan:** You've previously provided some super good information about cyber threats and what constitutes a cyber threat. What are some things that we should be aware of regarding the deliberate threat actors?

[00:18:01] **Randy Purse:** I think some of the things around cyber threat actors is we need to be cognizant that every minute is supple. Every CIO, every CIO, and every municipality across Canada should understand what the potential threats to their organizations are.

It's also the critical infrastructure across the municipality that they have some sort of responsibility to either manage, oversee, coordinate, or contract to third party services, to understand what those threats are and how they are tied directly to what risks you actually have.

The biggest I think mistake is under underestimating these deliberate threat actors.They tend to be highly motivated to attain their goals, whatever those goals are, almost always they're nefarious and criminal.

We've talked to a number of municipal leaders and as CEOs, and in general, they understand the problem and threat, but think they are too small and too insignificant to be targeted. But, there are a number of different threat actors who don't really care about your size.

There are many readily available online resources for these threat actors. For instance, ransomware as a service is a huge immerging trend, and there is a tool now online where you can go and you can buy ransomware for a very low cost and get it into organizations using phishing or social engineering techniques, with little to no technical expertise.

With a little bit of security, you can actually deny them the opportunity, which will likely detract them from penetrating your organization further. They're not going to spend hours and hours when they know there are organizations out there with little to no security measures that they can more easily target. Most of the criminal intent here is to do it quick, fast, get in, get your stuff, and leave. They don't want to be lingering too long.

So a little bit of security, goes a very long way.

[00:22:36] **Tenielle Bogdan:** What are some tips you can offer municipalities that would help them to better be prepared to respond to these cybersecurity incidents and threats?

[00:22:54] **Randy Purse:** The first one is ensuring your employees are educated on what your potential cyber threats are and what they can do about it. There is a huge talent shortage currently in Canada in the cyber space, so municipalities may not have the time or resources to hire a dedicated cybersecurity expert.

If employees know what to do when they think they've encountered a cyber issue, the more secure your organization is.Whether that may be just a call to the help desk or reporting it to their manager, or actually calling it into the cybersecurity center, they need to know how to do that but first knowing how to detect it.

What are kind of anomalous issues that may come up, whether it be in an email or the computer slowing down, or applications popping on my screen, they need to feel like they can report that easily and who they should report it to.

[00:29:15] **Tenielle Bogdan:** And that leads us to a great time to plug our Municipal Cybersecurity Best Practices, Guidelines, live on the TECHNATION website. It's a super simple, basic high-level document that talks about basic functions that municipalities can undertake and general awareness of things that they should know within their organizations

In talking about cyber hygiene, is there any resources or anything you can point the listeners to?

[00:29:55] **Randy Purse:** There are an awful lot of resources out there, which could be found with a simple search for “Cyber Hygiene”. There are resources within the Government of Ontario, the Canadian Centre for Cybersecurity, and through the Rogers Cybersecure Catalyst. The biggest thing I think is that you are using credible and reputable sources.

There are many resources and places to go, but I would start with the Canadian center for cybersecurity. That's my go-to place. The other, the other one is the National Institute for Standards and Technology (NIST)in the US. They have a cybersecurity framework, but it's incredibly involved and you need to understand some things in the cyber domain before you go launch and off and implement their framework within your municipality. But if you're a larger municipality is absolutely worth your while to go and take a look at them.

[00:32:49] **Tenielle Bogdan:** If you could provide our listeners with one piece of tactical advice that they could take away and implement today in their municipality, what would that be?

[00:32:58] **Randy Purse:** Leverage your people. So again, going back to the first statement about, how everybody gets all wrapped around the axle because the believe cybersecurity to be a technical problem while its truly a human problem, it's a human problem.

We have a number of resources available to municipalities, but there are some really simple things that you can do that are non-technical.

The first is, as we've already discussed, put in proper governance, and understand our team’s assigned roles and responsibilities. Secondly, do employee training and manage physical access to your systems, activate local software, and, do an asset inventory and categorization. All of these things take very limited expertise.

If you leverage your existing workforce, and instruct your existing people to do these types of things, you've already elevated your security posture a whole bunch, and you haven't even need to hired one cybersecurity expert.

You could do a lot of other things – you can put in VPN, you could put in automated patch management, which can be relatively inexpensive, which will significantly reduce your, your incidents. Cybersecurity incidents implement more rigorous pass access controls and password management,multi-factor authentication, eliminating administrative privileges. These types of things can be done with little to no expertise needed.

So again, it's about leveraging your people, taking what you have and seeing what you can do the best the most withbthose folks.

[00:35:18] **Tenielle Bogdan:** That's awesome. You heard it here, folks. Leverage your teams. Awesome. Thank you so much Randy!

[00:35:23] **Randy Purse:** No problem. My pleasure.

[00:35:27] **Tenielle Bogdan:** Big, thank you again to Dr. Randy Purse for chatting with us and sharing his knowledge around cyber attacks and incident management, as well as providing cybersecurity solutions for municipalities with limited budgets. To get connected with Randy or the catalyst head to www.cybersecurecatalyst.ca and check out their training programs and to learn further about how you can safeguard your municipality.