Cyber Safe Cities Podcast

10 Questions to Ask to Secure Your Municipality with Ruth Promislow, Partner at Bennett Jones LLP

[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 Ruth Promislow, Partner at Bennett Jones LLP.

Ruth has over 20 years of experience in litigating complex commercial disputes in a wide variety of areas, including privacy, cyber security, fraud re-insurance and professional names. She has extensive experience with data protection, privacy and cybersecurity matters, including regulatory compliance, cyber preparedness, breach response, and related litigation.

Ruth works with clients to assess their risks and vulnerabilities as well as their legal obligations regarding management of personal or confidential information. Ruth assists clients in developing comprehensive policies, guidelines, and procedures. To minimize exposure from potential attacks and to ensure compliance with regulatory and contractual obligations, following a cyber attack or privacy incident. Ruth oversees, forensic investigations and assists clients with regulatory investigations, reporting to regulators and providing notification to impacted individuals.

Ruth is also involved in all aspects of litigation, which may arise as a result of a cyber attack or privacy incident. Ruth is widely considered to be a thought leader in the data protection and privacy space and is an active member of the Sedona Conference, participating in the drafting of highly influential legal papers on privacy matters.

She was recently appointed to the steering committee of the privacy working group of Sedona. Ruth is also a member of the steering committee of the Canadian cyber security for. In this episode, we chat with Ruth about 10 key questions that every municipality should ask their team to ensure they are ready for a cyber attack.

We are so happy to have Ruth there with us today. Ruth, tell us a little about your role at Bennett Jones.

[00:02:31] **Ruth Promislow:** I'm a partner at the firm and I co-lead the cybersecurity breach response group, as well as the privacy and data management.

My practice is varied, so Ideal with so many things under the umbrella of cybersecurity, privacy, and data management, including breach preparedness, breach response, regulatory, and litigation issues, as well as transactional matters.

[00:02:57] **Tenielle Bogdan:** Let's chat a little bit about how incident response plans apply to municipalities and how they can help them be more secure.

[00:03:10] **Ruth Promislow:** Incident response plans apply to every organization, regardless of what kind of information or assets they have. It's no different than having a fire escape plan. You need to understand what you would do in a step by step for your worst case scenario.

And the reality now is that these are not unlikely events. They are likely events. And so all the more necessary to be prepared and understand precisely how you're going to respond. What everyone's respective role is in that response and templated responses for how you will deal with certain scenarios.

[00:03:49] **Tenielle Bogdan:** Can you explain how legal risk applies to cyber situations and what municipalities should be aware of?

[00:03:57] **Ruth Promislow:** There are several issues to consider in terms of legal risk rising from a breach and the management of the breach. Firstly, you don't only have exposure for the breach itself. You can have exposure for mismanagement of the breach in how you respond and manage the breach. What you say can be used in litigation or regulatory investigation against the municipality. For example, any press release you issue following the event could be used as evidence that you've acknowledged and you've fell below the standard of care.

Those are a couple of examples. There are several more in responding to a breach and often messed up, which we'll probably come to this in a bit more detail later. Not just municipalities, but organizations to destroy key forensic evidence in the course of trying to contain the incident and manage it.

And in doing that, they really do themselves a disservice, and everything becomes more costly and less certain because without that very important evidence, you can't get to the bottom of the breach. Where did the intruder go and what did they do while they were inside your network?

[00:05:25] **Tenielle Bogdan:** You raised an interesting point on how you respond toa breach could potentially affect your legal risk. Can you chat a little bit more about that and the duty of care?

[00:05:36] **Ruth Promislow:** There's several things to think about. You have a duty of care. Once you have custody of information, for example, you have an obligation to safeguard that information using reasonable steps. You also have an obligation to notify individuals where there is a real risk of significant exposure. And you need to do so in a timely way so that [00:06:00] these individuals can take steps to manage any potential exposure to them, such as identity theft or other forms of fraud by failing to give individuals that notice in a timely way.

Likewise, when we're talking about municipalities, we're also dealing with essential services and critical infrastructure. We're dealing with human safety issues, not just personal information. We have credit card information that someone may get their hands on. Municipalities have such a broader spectrum of risk when talking about cybersecurity. It's not just information being stolen, there are also integrity issues. People rely on the integrity of an municipalities information system, like marriage [00:07:00] licenses or real estate or taxes.

I mean, these are really important things. How do you know that these are accurate records? You need to have a system in place to be assured of integrity. Likewise, when we're dealing with essential services, you want to know that you have safeguarded your system so that when people are calling for essential services, are coming in to the appropriate people. They're not being diverted and you are responding in a timely way.

It's odd, but I'd say municipalities in my experience tend to devote fewer resources to these issues than commercial organizations that are really just safeguarding information and don't have such an important role in public safety.

[00:08:02] **Tenielle Bogdan:** How does legal risk and reputational risk come into play when we're talking about things that you should share in your communications plans? How you should engage your communications team in dealing with these types of incidents?

[00:08:15] **Ruth Promislow:** I'm a big fan of transparency. I think transparency wins a lot of points. People really value being told early on what has potentially happened or what has happened. But at the same time, you can be transparent without acknowledging liability.

And there's a very delicate balance. Communication experts and lawyers often we have the back of a back and forth where we're drafting and we have different objectives in how we draft certain statements. [00:09:00] And at the end of the day, you really want to make sure that you're listening to external council's advice on those messages, because

certainly you want to make people feel calm. You want them to know you're being responsible and responsive, but at the same time, you should not say anything that improperly acknowledges liability and exposure. It's a very delicate balance.

I think a takeaway on this particular discussion point is how important it is to have different perspectives incorporated into your decision-making. When you're preparing to respond to a breach or responding to the breach, these different perspectives are very valuable. If you only take into account one particular perspective or expertise, you're not helping yourself in the best way that you can. In your communications strategy, I think it's important to have all the different players at the table to voice their views on what is best for at the end of the day.

[00:10:16] **Tenielle Bogdan:** And in chatting about those communications, do you have any suggestions or recommendations on who should be the spokesperson or who should be leading the charge in this messaging

[00:10:31] **Ruth Promislow:** Well, I guess the broader question there is who should really sort of take charge on the breach response strategy. I think it's very important that it come from senior levels. There could be different people who play that role. And in my work with municipalities, there are various roles or players that I've dealt with, but it's so important that you have someone at the senior level.

I often find it's important to [00:11:00] have either the CFO or someone in the senior levels of finance, because there are decisions being made about how you manage exposure to risk. The CFO or someone working closely with the CFO needs to understand if this plays out and we don't do employ this strategy, the cost is going to be X. And in these are things that you need to really map out in advance. Likewise, I think people from HR, from operations, from IT, and from compliance. These are all the different perspectives that need to be brought into play.

[00:11:56] **Tenielle Bogdan:** Let's circle back to, to what we're talking about today, and those are the 10 questions that every municipality should be asking their teams. So there's obviously different areas that we can be focusing on, but what would you say is the main priority question that municipalities should be asking?

[00:12:12] **Ruth Promislow:** At a very high level, what these questions are designed to do, or to focus the attention of the municipality on, on developing a risk management strategy. What that involves is understanding what are our risks. What are our worst case scenarios? How do those risks, those worst case scenarios, unfold? What would be the cause of each of those different worst case scenarios? What is the potential damage or cost to each of those worst case scenarios? And how can we minimize the likelihood of those event, or the potential impact of them? That at a high level is what you're trying to do.

I come back to all the different perspectives because often I get involved and I start dealing with someone within leadership and the municipality, and they delegated the management of this risk to the IT team that's it. This is a bad strategy to delegate IT entirely because it brings one perspective, not the entire perspective. They can tell you how they can manage the risk from an IT perspective, but IT doesn't manage the people within your organization.

I think the best piece of advice I could give to municipalities is assemble a team, a cybersecurity team with team leaders from within all the different divisions.

If you put together a team and mobilize your internal resources, you were going to be far better off than you are right now. And you don't have to spend a lot of money on this because your internal team will get very far and then you'll have a very concrete risk management strategy. That's when you can consult with external experts, you keep your costs way down with a lot of the ground work already done.

And if you've gone to all the work of assembling this team and putting on paper, all the components that I've outlined and mapping out your strategy, you have a defensible position that you have taken a reasonable steps in light of your available resources.

[00:16:23] **Tenielle Bogdan:** That's awesome. I love the idea of starting somewhere. I'm sure that you've seen with your experience, some overlap as well between those teams of one department might be dealing with one thing that could be similar to another one and where we're breaking down those silos within the organization.

[00:16:37] **Ruth Promislow:** When you work in isolation, they don't realize the commonalities within your different teams. HR and IT don't always talk just as an example. So HR makes a decision to terminate employment for some reason, but they don't tell IT necessarily, or they don't have a protocol that says, when you terminate an individual, they looks access to the systems through IT. I've seen scenarios where the disgruntled employee goes back to their desk and wipes information because they're angry or they download information. That's just an unnecessary risk. So if you have this team and you've tasked them with developing this risk management strategy, that would be one of the risks that they would identify, and they would identify a method to manage that risk, which would be here's a protocol HR, every time we were about to terminate, you have to call this person in it and notify them so that they can disconnect access.

[00:18:01] **Tenielle Bogdan:** When should a municipality look to engage their legal team in incident response?

[00:18:07] **Ruth Promislow:** I think there's a rule we (your legal team) can play once the team has developed this risk management strategy and an incident response plan.

We can provide our high-level view and comments and guide them on certain key things they may be missing and to also make the connection so that they know who to call and they pick up the phone quickly. I think one of the biggest missteps I observe across the board with municipalities and other organizations where they try to manage the incident initially on their own, because the thinking is “I don't need a lawyer. I don't have legal issues yet.” You have legal issues as soon as you learn about the event and too often, there's a damaging paper trail or privilege is lost and legal privilege is very important. It's intended to protect communications that are undertaken for the purposes of informing council, so that council can give an opinion or advice.

So for example, the forensic expert work a certain part of IT is properly protected by privilege. Not all of it is can always be protected by privilege, but a certain part is. Often the municipalities will have already directly engaged external forensic experts, and that would not be the best way to approach things.

The better way is to first engage counsel to structure the engagement of the forensic experts. This ensures that privilege is best protected and to guide the municipality on the internal communication so that they're not creating an internal paper trail, likewise, to guide the municipality on their external communications and what they're saying to third party. What they shouldn't say and what they shouldn't say, because there are third parties that you may not have a regulatory obligation to notify, but it is often a good idea to notify them, to manage risks. What are our potential sources of exposure and how do we manage that?

And that's what lawyers do. I mean, that's our bread and butter. So that's where, when we get a call, we can very quickly sort of look at the incident and say, here's where your potential exposure is. Here are the people who can potentially come back and make a claim against you. And let's look at how we can manage that.

As soon as you know you have an incident, pick up the phone and call counsel with expertise in this area. But even before, it's good just to make the introductory connection, to have us review your risk management strategy and your incident response plan.

[00:21:24] **Tenielle Bogdan:** Where do you think is the best place for municipalities to start assessing their risk?

[00:21:32] **Ruth Promislow:** The best place is start is toassemble that team and have them start looking at those very high level issues and really teasing things out.

And as you mentioned in your opening questions, the third party risk, I mean, this would fall under a broad heading of what are our worst case scenarios and how will they occur very frequently. Everyone forgets third party risks, so that if a third party provider is compromised, how does that impact us?

Do you have the provisions in agreements with your third-party providers that protect yourself? Are there any missing provisions? Just for example, obligation on a third party provider to notify the municipality within a certain period of time of any incident with which they suspect may be material, how quickly they have to notify, whether you want that third party to have insurance too.

There are many aspects when you really get down to what the risks there are. It's not just, “okay the risk is a ransomware attack.” You need to break it down. What happens if there's a ransomware attack? What are the integrity issues? What happens if you can't access your network? It's a lengthy. detailed process. I would stress that there's not an off the shelf playbook to help you identify these issues, but there is guidance.

So I think just in terms of what municipalities can do right now, I think number one is assemble that team. Give that team a mandate, give them a sort of an outline of what you want them to accomplish, how frequently they should meet and what their deliverables are. I suspect that you get pretty great results.

You cannot manage a risk without understanding what the risks are. And there's no way to really have an effective strategy without knowing your risks.

[00:24:39] **Tenielle Bogdan:** Are there any policies or any tools that you think municipalities should be aware of in transitioning from traditional offices to a bit more of a hybrid model?

[00:24:49] **Ruth Promislow:** There's some important issues to consider there with that very rapid transition that we all went through because people, like organizations and municipalities alike, were not ready for it.

Of course, you have individuals working from personal computers. That can be an issue depending on the role of the individual within the organization and the sensitivity of the information or assets to which they have access. That's much harder to control than if you had devices that were issued by the municipality or the organization to the certain employees. Something that I encourage a lot of clients is to carefully consider providing your employees company-issued equipment because it’s much easier to control. It would be very easy for a bad actor to do real damage very quickly. And once you identified those people, it's a much lower cost to give those people a laptop to work from home than to just assume that risk.

You need to understand what the costs are. Put dollar amounts to these costs because once you start mapping out your risks and what are the dollar value cost to these events, buying a laptop for a few employees is going to seem like it's penance because it's nothing compared to the millions of dollars you could have to spend to rebuild your network or to provide identity theft protection to individuals because their social insurance number was compromised.

In terms of the software, understanding and making sure that all patches are applied and that you can remotely wipe the device. What if an employee says, oops, I lost a laptop I use for work and I hit downloaded a bunch of sensitive tables onto my laptop with important information cause they were going to work offline. You need the ability to wipe the information on that laptop remotely.

If it's a personal device, very sticky issue about, can you inspect their personal device? It's very difficult. If it's a work issue device, you get to say, bring your laptop into the office this morning, please. And that's when you deliver it, you know, that that's maybe when they find out that they're no longer employed.

[00:28:47] **Tenielle Bogdan:** How does that apply to personal mobile devices? I know there's a lot of organizations that will have a work phone but do work off their personal device.

[00:28:55] **Ruth Promislow:** It is absolutely similar issue because you really need to think about what the risks are in terms of remotely accessing information or assets from your personal device and the ability of the organization to wipe your device or to require that you turn your device in to be reviewed. These are the same sorts of issues that I think they just became magnified with the work from home structure, because typically on your personal life, you can access email, but maybe you couldn't access sort of the accounting software that the municipality uses, but from your laptop, you can, and now you have this person on their home computer where, there children and spouse may use the device. Once you add on users to a device, you add on risk.

So to the extent municipalities have not really given thought to that element of the cybersecurity. It's very important to task your cyber team with that question, as well as HR.

[00:32:01] **Tenielle Bogdan:** Let's chat about insurance. What are some trends that you're seeing, or shifts of trends, in terms of insurance?

[00:32:08] **Ruth Promislow:** One of the most interesting developments that occurred, was when one of the insurers in France announced that it would no longer provide coverage for ransomware payments. I think that's been a very hot topic of discussion within the cyber insurance market. We haven't seen others follow suit, but it certainly will. I wouldn't rule it out that the actual ransomware payments may not be covered in the future. But I think that the general discussions are that there's a contraction of the types of events that will be covered and an increase in premiums, or at least an expected increase in premiums.

When you look at insurance, the idea of insurance is to insure against unlikely events. And cyber attacks are becoming likely. I think insurers are taking a very hard look at this because they not going to issue the similar trends that we've seen over the last few years in the market.

That's really been driving the sales and the interest in cyber insurance. I think we're going to see very different structure and organizations should not make insurance your main risk strategy. That can be an element of your strategy, but don't assume that having coverage for a ransomware payment is all you need. Cause that's the assumption is that the bad actor will actually give you back your data. We'll decrypt your whole system in exchange for the ransomware payment, which that's not a safe assumption. So I think the insurance market is going to change. I think there's, there's a lot of movement and I think maybe the insurance market will actually play an important role in improving cyber hygiene in terms of requiring an elevated level of preparedness as a condition for underwriting the risk. That can be a very positive impact that there'll be sort of better guidelines on how organizations should prepare for this risk

[00:34:35] **Tenielle Bogdan:** If you could provide our listeners one piece of tactical advice to take away what municipalities

[00:34:43] **Ruth Promislow:** Look to all the available resources to you in cyber security. Because they are there organizations that are there to support municipalities in their work and addressing cybersecurity risks. TECHNATIONis a great example.

I also think they probably can help each other and have these discussions and learn from each other's experiences. Because every time I work within a municipality in handling a cybersecurity event, they come out stronger. They know something they didn't know before, and they're better off and they can share that knowledge and that experience.

One of the items on your internal cyber team's list should be to identify all the external resources available to us from which we could get helpful tips and hints about how to manage these issues because your team is going to look into it and come out with a very helpful. Of those resources and then you can start to lean on those at no cost.

[00:36:56] **Tenielle Bogdan:** A big thank you to Ruth and the Bennett Jones team for being part of this initiative and sharing their insight and expertise. To get connected with Ruth and her team at Bennett Jones. Head to their website www.bennettjones.com or check out the link in our description of this episode. Thanks for tuning in.