Cyber Safe Cities Podcast

Working with Law Enforcement with DS Vern Crowley, Ontario Provincial Police

[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 Detective Sergeant Vern Crowley with the Ontario Provincial Police.

Detective Sergeant Crowley is a member of the Ontario Provincial Police's Cybercrime Investigations Team, which is comprised of police investigators and civilian technical experts. The team's mandate is to investigate cyber crimes where technology is the target of the crime, assist in complex criminal investigations where technology was used as a tool to commit the crime, and to work collaboratively with law enforcement, government academia, and the private sector to enhance cyber intelligence sector.

Detective Sergeant Crowley chats with us today about how municipalities can work with their law enforcement once they have experienced a cyber attack.

Hi Vern! Thanks for joining us today. Tell us a little bit about your role with the OPP.

[00:01:44] **DS Vern Crowley:** I'm a 30 year plus sworn member with the OPP. The majority of my time over 25 years has been dealing with digital evidence-based investigations.

Currently I'm assigned to the OPPs Cyber Crime Investigations team as the outreach manager. My responsibility is building those partnerships with both the private and public sector to share threat intelligence and help harden Ontario IT networks with the goal of reducing the victimization that's caused by cyber crime within the province.

[00:02:16] **Tenielle Bogdan:** In what capacity have you been involved with municipalities and their cybersecurity?

[00:02:22] **DS Vern Crowley:** I've been doing this for a very long time, almost a dinosaur, if you will, when it comes to digital technology and criminal investigation. I started investigating criminal offenses back in 1995, starting out as a computer forensic investigator. In 2015, I assisted the OPP in their cyber strategy, which was a holistic look at our organization and how we deal with technology and digital based evidence.

One of the things that that came out of that was the need and capabilities within the Ontario Provincial Police to actually investigate cyber crimes. Out of that, I became part of the team. Currently, I'm the Outreach Manager because we came to realize very quickly, especially when it comes to cyber crimes, that we can't do it alone.We need to build those positive working relationships to assist in targeting and hardening Ontario, and do our role, which is to catch the bad guys that are doing cyber crimes.

[00:03:22] **Tenielle Bogdan:** We know that cyber crimes and attacks are happening all the time and threats are increasing for municipalities. But one thing that our listeners might not know is what the protocol is for engaging their local law enforcement.

So when should a municipality engage with law enforcement when dealing with a cyber attacker?

[00:03:40] **DS Vern Crowley:** That's a great question. And I'm glad it's part of this podcast. The best practice, in my opinion would be to reach out to your local law enforcement before an incident even happens to find out what the reporting protocols are, and build that positive relationship so that when an incident happens all parties are familiar with one another. If the local law enforcement does not have the capability or capacity to properly respond to that cyber incident, they will reach out to us as the provincial police service, our cyber crime investigation team.We will work with that local law enforcement agency for the appropriate response and resources, no matter where the victim is within the province.

Now, one of the key issues is we need to know as soon as possible, the details of the cyber incident or the cyber attack and the impact that it has on the organization. If we can get those details, as soon as possible, this will allow us to better assess the situation and collaborate within our law enforcement committee. If there's one thing I can say within the 30 years in policing, I have never seen such great collaboration amongst law enforcement agencies. When it comes to cyber crime, we are doing a great job of that.

I can tell you, I am literally on the phone weekly with our new municipal partners, federal partners, and international groups, be it, the FBI Homeland security or NCA. We talk about the different cyber threats and the different cyber crimes that are happening. So that quick and timely notification allows law enforcement to attain the proper resources required to respond effectively.

It also allows us to gather that information, which would lead back to linkages to other possible investigations. Rest assured as a victim, you are not alone. This is global. Quick reporting will allow us to link up to other investigations and the lessons learned from those incidents may be able to be shared to speed up the appropriate mitigation and remediation efforts for the victim organization here in Ontario.

[00:06:01] **Tenielle Bogdan:** Knowing that you have an Ontario focus, can you comment on whether or not the process is similar for other provinces and territories across Canada?

[00:06:12] **DS Vern Crowley:** We're kind of fortunate that we do have that provincial entity but in working literally across the province, as I said there, we can't do it alone.

We are in contact with our law enforcement partners coast to coast, as well as the RCMP who has a federal responsibility. So for all the government network services and critical infrastructure, the RCMP is going to be the police force with jurisdiction, who will work locally again with the law enforcement community.

Some local law enforcement agencies are a little more mature than others. But we are all learning and we all support one another. So again, the most important thing is to reach out in advance, find out what the capabilities and the reporting protocols are, so that if and when something happens, you know the proper steps to take.

[00:07:21] **Tenielle Bogdan:** You touched on how law enforcement can help in bridging and connecting cyber incidents that happen across the global landscape and a national landscape. What else can law enforcement do to help in dealing with these types of attacks?

[00:07:34] **DS Vern Crowley:** As law enforcement our main responsibility is finding out who committed the crime, the mitigation or remediation, and the negative effects of the event. How to get the IT systems back to where they were before the attack is the responsibility of the victim organization. The timeliness of the reporting is super important for law enforcement.

Some of those lessons learned from those other victim organizations, we may be able to present to you. If we're able to present those best practices that helped mitigate another event, this may help your remediation process can go more efficiently. Its almost guaranteed that if you're a victim organization and you go through this, you will not want to have this happen to your neighboring municipality or your neighboring organization. Tt's a horrible thing to go through.

These cyber criminals, unfortunately, are making a lot of money at doing it and they continue to do it for two main reasons. One, it's generally not being reported. And two, they're making lots of money when it comes to ransomware or holding your data hostage. So there's low risk for them doing it. They're making lots of money, high gain, low risk. Why would they stop? And it's one of the, that's the main reasons why it's happening and it's so prevalent today.

[00:09:16] **Tenielle Bogdan:** What pieces of information should municipalities have ready when working with law enforcement?

[00:09:28] **DS Vern Crowley:** Make sure that the person that's going to report the incident to law enforcement is well aware of what has happened, the effects and the level of jeopardy that the organization is facing.

The timeliness for these crucial pieces of information is super important. So the person that's reporting needs to have firsthand knowledge of the incident and the overall effect on the organization.

And then really a cyber crime is no different than any other crime. If you were to put on your police hat and pretend you're the police officer, we want to know, you know, the five Ws: who, what, where, why when.

The very first things that we will want to know, as I mentioned before is, you know, what has happened, what is affected and what is the level of jeopardy. The type of things that we would want to know in the case of an encryption, you know, what would the file extension be? Because that gives us a better idea of maybe what it is that they're looking for. So that's crucial as well. We also would want to know what steps have been taken. Sometimes it's the IT department along with a third-party security company that they have brought in. Sometimes it might be a total third party that was brought in through cyber insurance.

Rest assured that we will work with the IT department and or the third party security company. We are not there to interfere, we are there to help.

We also want to know is there is an ongoing threat or concern. If the incident is over and stable, that’s great. But if its two or three weeks after the fact, we need to know if there is implications on operations or public safety, because that is going to be a number one concern.

So once the incident gets reported, how can you best supplement back reporting? What pieces of information do we have? The basic details in relation to the incident is what we need. Law enforcement will want to preserve and gather any potential digital evidence related to that cyber incident as soon as possible. So things such as log files, suspicious logins, IP addresses, applications, or processes that were running that are suspicious, as well as any identifiers of the threat actors. So that might be monikers, email addresses. The bad guys use these anonymous emails. It could be proton mail or different domains, Bitcoin wallet, IDs. If it happens to be a ransomware, that's going to be absolutely important. Any communications that they may have had be it, the ransom note, if it was displayed on the screen, or if they had sent you an email or even telephone calls they need to, the telephone number that he came from. The contents of those communications would be great, in addition to any suspicious files.

We'll probably always ask the question. Who do you think may have done this? They'll the incident may appear to be from an external threat actor. One can never really rule out an insider may have played a role to some extent, and again, our job is to make sure that we have full knowledge as best as we can for the incident.

[00:13:56] **Tenielle Bogdan:** Is there any other departments that you would say you work most closely with in dealing with incidents?

[00:14:11] **DS Vern Crowley:** First and foremost, we work with the victim and we work alongside their IT departments. Often, there's a lot of fear. And maybe this is some of the reasons why law enforcement may not necessarily be notified right away.

One of their fears may be that law enforcement would come in and hamper the mitigation and remediation efforts, which is not true. We want to reduce the level of victimization that's caused. So we'll work alongside the organization. Another fear is maybe some of the information may be leaked to the media or the media will be notified. That is also not true.

Since it's a criminal investigation, we would never comment on it or divulge information. Some also might fear that the police might be sensitive information or third-party data and hand over the information we collect. As mentioned before, law enforcement deals with the incident itself, the metadata and necessarily the contents of the database or any financial information.

Another stigma is thinking that there is no benefit in reporting the incident to police. Teams like the OPP Cybercrime Investigation Team have built capacity and are making headway in catching the bad guys. So there is a lot of value in reporting to the police.

Other agencies provide support such as the Canadian Center for Cyber Security (CCCS), who is not law enforcement. Because of where they fit within the Canadian government, they're not really allowed to share anything. So if someone were to report to the CCCS, the information is not necessarily shared directly with law enforcement. More than likely the CCCS will encourage you to report the incident to your local law enforcement, so it is important that you do so.

I would say that proactive step for people that are listening to the podcast, is to find out where those resources are and that'll help you long on your way to get your incident response plan together.

[00:16:51] **Tenielle Bogdan:** Are there any other external partners or third-party vendors that should be engaged during the process of working with law enforcement?

[00:16:59] **DS Vern Crowley:** We'll probably have cyber insurance of some form. Upon an incident happening, the cyber insurance company will deploy those companies and resources that they have in a retainer to quickly respond to the incident. We have incident response, digital forensics, legal counsel, marketing and or reputation firms. And they'll all be standby. Quarterbacked by the insurance company, they will work with any of them. Again, it's working with them to allow the sharing of information.

One of the cautionary tales, or one of the notes that I want to bring to everybody is that often a breach coach or legal representation may ask you the victim to delay or even avoid law enforcement involvement to protect the interests of your organization. But adding to that reluctancy to report is really a negative thing. You have the right to report like a break and enter. If police don't know about it, it becomes very prevalent and continues all the time.

[00:18:16] **Tenielle Bogdan:** You mentioned the Canadian Center for Cyber Security and the differences between your two organizations, but how do you guys work together to fight cyber crime?

[00:18:24] **DS Vern Crowley:** We work with them. Their main mandate is to support critical infrastructure, which includes municipalities across Canada, increas cyber resiliency, and also to promote the reporting and if possible, able to provide guidance to help them do the proper mitigation or remediation.

That's where we compliment one another. We work together to try to reduce the victimization that's caused by cyber crime. So a lot of times CCCS may be put on informative webinars and they'll reach out to us for a law enforcement perspective and then vice versa.

[00:19:33] **Tenielle Bogdan:** We know that the threat landscape is increasing rapidly. Would you say you've seen any trends within the pas two years?

[00:19:42] **DS Vern Crowley:** Ransomware has been the scourge of municipalities specifically, but also the healthcare industry. Crime groups that getting much better with ransomware. They're not discriminatory. Wherever they can get the money, that's where they're going to apply their criminal malware into systems and, and hold you up for ransom. Ransomware has probably one of the highest level of jeopardy in that once they get into the network and it could be through a remote desktop protocol, could be through a phishing email, or a malicious attachment or malicious link.

Once the criminals are in, they move laterally and they scour all your relevant data. First, they'll try to steal it and then they'll encrypt it, demanding Bitcoin, more than likely for payment. They will put added pressure for the payment that they will disclose, either on a leak site or by literally notifying your stakeholders and or the customers of the records that they've obtained and tell them that they have your data and that it will be released.

So now the victim company or organization or municipality has members of the public, or their stakeholders, all putting pressure on them that do something about this because we don't want their records out there.

We've seen within the past 12 to 18 months our critical infrastructure is being probed a lot more. There have been some incidents you've heard about the colonial pipeline in the United States, JBS, which was the meat packing distributing, which actually affected the supply chain within Canada as well.

We are seeing now that these key pillars within our economy, be it under municipal control or elsewhere. now being probed by the cyber criminals. We must take care and do our due diligence to make sure to the best of our efforts that we secure it.

[00:22:07] **Tenielle Bogdan:** And we've heard a lot about the crimes of opportunity. Are you still seeing that as prevalent in cyber or cyber criminals? Are you finding that cybercriminals are trying harder to get into the systems or merely taking the easiest opportunity for entry?

[00:22:20] **DS Vern Crowley:** It's a combination of both. They're very opportunistic. So everybody in the here and now the timeliness of this podcast here in Canada, we're going into another lockdown

So be prepared. Cyber criminals are going to apply their social engineering to trick you into clicking or getting more information. Back in March 2020, we saw the cybercriminals switch and focus. We just had a disaster in Haiti. So anytime that there was a relief effort, they will put their social engineering skills and ramp up.

The whole campaign for the Canadian anti-fraud center, "think before you click" is a great campaign

If you do not have one, now is the time to create an incident response plan and make sure law enforcement notification is a priority within it. Reach out to your local law enforcement agency and see what those reporting protocols are to build that positive relationship before the incident actually happens.

[00:24:17] **Tenielle Bogdan:** That's fantastic. Thanks Vern.

A big, thank you again to Detective Sergeant Crowley for sharing his insight and expertise in dealing with cyber attacks and things municipalities should be aware of when working with law enforcement.