Understanding and Addressing Ransomware Threats

Speaker:
Colleen Merchant, Director General, National Cyber Security, Government of Canada

Session Moderator:
Dafna Carr, Associate Deputy Minister and Corporate Chief Information Officer

Dafna: Hello everyone, and welcome back.

I know that you've been doing some networking and I was listening into the panel before.

Terrific opportunities to learn from some excellent experts out there, and thank you Charles, for the moderation.

Now, we're back to the agenda and I'd like to welcome Colleen Merchant.

She's the Director General for National Cyber Security, Government of Canada and Coleen's career spans over 30 years and includes the Canadian Space Agency, the Communications Security Establishment of Canada, CSEC and the Treasury Board of Canada Secretariat.

So, welcome Colleen and over to you.

Colleen: Thank you very much.

I'm really pleased to be here and especially talking about something that I think is affecting most of us, which is the ransomware issue.

So, if I could have the first slide, I'll dive right in.

Defining ransomware, the Canadian Centre for Cyber Security has defined it, you can read it there.

A type of malware that denies access to a system or data until you pay a ransom.

And unfortunately, it's the most widespread and financially damaging form of cyber attack in the world today.

There was a study interestingly enough, that showed that Canadian companies are more likely to pay ransomware demands than businesses in other countries.

And it showed that 75% of Canadian companies would pay a ransom after an infection, as compared to only 3% of US companies.

And I have to say, it's still unclear as to why Canadian businesses are more likely to pay than their counterparts, but that's something obviously that we need to follow up with.

We've seen a recent trend and that is that ransomware attacks are increasingly targeted.

Targets are selected for their ability to pay ransom or the probability that they'll pay, instead of these attackers who used to be targeting individuals and businesses doing so indiscriminately, they're now able to look with a little more targeted aspect.

So, the attacks are more targeted toward lucrative businesses, as you might imagine, that's up 12% and are made more profitable as the attackers then demand a larger ransom and that ripples into a much larger damage to the economy.

A study that surveyed organizations in 11 countries found that the average annual cost associated with resolving a ransomware attack per organization was about 645,000 US dollars in 2018, and that was up 21% from the previous year.

Next slide please.

In terms of the evolution of ransomware attacks, the techniques that are involved in the execution of a ransomware attack are evolving.

In the past attacks followed a pattern of one, compromising the victim systems weeks, and sometimes months in advance of actually launching the ransomware.

And this would allow the attacker to target the most profitable data of which to encrypt.

Then launching the ransomware attack by specifically encrypting those targeted files.

And then once those files were encrypted, demanding a ransom, ordering the victim to pay a fee to unlock the data.

So, attacks have now advanced so that the ransomware payloads can often be delivered within a week of compromising the networks, which reduces the

amount of time to actually detect that there's an issue within the system.

Additionally, attacks have really diversified in the consequences that they'll deliver, and I'll give three examples here.

One, data theft, so cyber criminals can either steal the data and then before encrypting it threaten to publicly release it if the ransom is not paid.

So in other words, blackmail, and they can also take the encrypted information, get the ransom money, but then take the data and sell it on the black market for even further funding or financial gain.

Another new impact is the actors that are targeting industrial control systems.

So, this is ransomware that specifically targets and interferes with industrial processes, so this causes a physical impact to critical infrastructure.

A third diversification is in destructive malware that's masquerading as ransomware.

In other words, the attackers don't intend on decrypting files once the ransom's paid, they're simply using this method to disguise another type of attack, whether it be espionage or another as ransomware to serve as a diversion or to complicate the attribution process.

These evolutions in attack methods and motivations really added to the complexity of the problem that we here in Canada are facing today.

Next slide please.

The Canadian context, the magnitude and frequency of events in Canada has been increasing and since fall 2019 recent ransomware attacks in Canada have included those on healthcare providers, crown corporations, provincial and territorial governments, law firms.

So, it show's not only the significance and the increase of number of attacks, but also the variety of targets that these cyber criminals will attack.

So, in 2018, Canadian businesses reported a rise in the frequency of ransomware attacks, despite an increase in global ransomware events.

As I mentioned earlier, a recent study had found that Canadian businesses were more likely to pay ransom demands as compared to other like-minded countries, which is probably what explains the increased frequency of attacks in Canada, as we're seen as a paying customer.

Obviously, that's very concerning as the prevalence of ransomware payments here in Canada is challenging deterrence efforts that the Canadian government and our law enforcement agencies are undertaking.

Granted, there are a variety of consequences in ransomware attacks on businesses, and these factors can compel businesses to pay ransom and create disincentives, such as reputational risk for businesses to report an incident to police or the cyber centre.

Next slide please.

So, recent events.

Attackers using ransomware are opportunistic in their efforts.

So for instance, in the wake of COVID-19, there's been a lot more exploitation of the health care and federal government services related to the pandemic.

Hospitals and health care providers have a diverse and vast amount of medical equipment that is connected to their networks.

Attackers know this, leading to increased ransomware attacks on hospitals and health care providers.

And given, in the current context, the urgency of the needs of the patients, you've got an increased probability of payments to get a quick fix and help those that are in need.

Threat actors have also created malicious websites under the guise of Health Canada in order to distribute ransomware designed to look like a federal COVID-19 contact tracing app.

And COVID-themed phishing e-mails designed to imitate federal governments, and federal departments and agencies, public health professionals, and workplace policy e-mails have also seen an increase recently.

Also, ransomware attacks have been directed at the return to school by students and teachers.

There are school districts that were affected by ransomware attacks on the first day of school, had to be closed down.

Also in recent weeks, there've been a few very high-profile ransomware attacks globally, including on BancoEstado, one of the largest banks in Chile, and the Argentinian government's agency responsible for immigration.

This one, I would like to note, is speculated to be the first known attack against a federal agency that has actually interrupted the country's operations.

Next slide please.

So, the complexities of ransomware.

If we're tackling at the federal level, these are the things that we really need to look at because the complexities are things that transcend borders.

Cyber attacks are borderless, and that generates additional challenges when networks and infrastructure are interconnected across municipal, provincial and territorial borders.

Federal leadership and coordination is required so that we can avoid serious consequences, which could happen if each victim is left to come up with its own response.

For example, I always use this one, electrical grids.

So, electrical grids are provincially regulated, but they cross provincial borders.

So, if you have a province that's hit by a ransomware attack, could that impact one or more other provinces and territories? And if so, who's involved and how, on a decision as to paying the ransom if there's an absence of an agreed-to framework.

So, that's an example of some of the questions that we're working to address at the federal level and hoping that we'll be able to increase our collaboration with our provincial and territorial partners on this issue in the future.

We all know that cyber attacks targeting critical infrastructure have the potential to cause significant effects, not only to the public safety of Canadians but to national security as well.

And ransomware attacks targeting critical infrastructure are no different as they could cause delays in the delivery of essential services and potentially cause destructive consequences.

Imagine an attack on the energy sector in the middle of winter or on telecommunications networks in the wake of a huge crisis.

So, this leads us to look at things like where a ransomware attack becomes an attack on our national security, and it would help determine what type of response would be necessary.

So in other words, how does or should the government respond to state-sponsored ransomware attacks? What if these attacks target critical infrastructure? Does the intent matter? In other words, whether it's these ransomware attacks are being done for financial gain, or to destroy critical infrastructure, or for political gain.

So, these are all things that the federal government is looking at.

Next, please.

Obviously, prevention, best defence.

So, investing in cybersecurity is something that is primordial in terms of making sure that you're as secure from ransomware as possible.

While the majority of Canadian businesses have invested in prevention or detection, cyber incidents, you can see from the chart on this slide, that these investments vary significantly from an average of $922,000 in spending by large businesses to 44,000 by small businesses.

The cyber centre is our expert on cyber security here in Canada, and Michele Mullen, my colleague there, will be talking to you, I think, in the next session.

But they provide recommendations on basic but very effective mitigation strategies to reduce the risk of ransomware attacks, namely security awareness training, patching, disabling macros, restricting admin privileges, performing regular backups and practicing through simulation how you would respond and recover.

Next slide please.

So, speaking of responding.

So, equally important to prevent in is how organizations respond to an attack.

And having recovery procedures in place and practicing those procedures goes a long way to limiting the impact of a ransomware attack.

Obviously, you wanna disconnect the affected device or devices from the internet to prevent any further spreading of the malware to other devices.

Then you wanna look at how you recover the data.

So, you restore an offline backup, are things in the cloud? And there's also the potential to use free decryption tools such as those in the online repository by the No More Ransom Project.

And there's a link to that project later on in the deck here.

So, Canadian law enforcement strongly advise against paying the ransom for a number of reasons.

Number one, doing so can make the organization vulnerable to future attacks because it demonstrates that the organization is a profitable target.

Number two, there's no guarantee that the cyber criminal is going to keep their word and that they won't ask for additional money, form of double extortion, or destroy the information, or publicly disclose it.

Third, the payment of ransoms can create serious legal risks if the attacker is associated with a sanction or listed entity, because giving money to a sanction or listed entity here in Canada is a criminal offence.

Finally, paying the ransom proves that ransomware works and it just generally encourages more criminal activity.

And we know that cyber liability insurance exists, and some coverage can include the costs associated with cyber extortion, including the payment of ransom.

However, we have to keep in mind that cyber criminals and targeted organizations known to have cyber insurance coverage because they're considered profitable and more likely to pay the ransom.

So, another piece of the responsibility is reporting.

We encourage victims of ransomware attacks to report the incident to their local law enforcement or the Canadian Anti-fraud Centre and the Cyber Centre.

Instead of paying ransom, invest in cyber security.

Next slide please.

So, in terms of the federal government, what are we doing? What have we done? So, the ransomware landscape has always been evolving.

The rapid pace of escalating risk indicates that this work is more critical than ever, as Canadians and businesses are increasingly turning to online solutions, in particular, given the situation with the pandemic.

Here's some of the steps that we've taken to protect Canadians from

ransomware and other cyber threats, including the development of guidance materials on how to protect systems, continuously removing COVID-19 related fishing sites that mimic Government of Canada sites.

We've launched the Canadian shield initiative.

That's a free protected domain name system, or DNS service, that prevents individuals from connecting to malicious websites that might infect their device or steal their personal information.

And we have established the CyberSecure Canada Program last year, a federal cyber certification program, that aims to raise the cybersecurity baseline among small and medium enterprises in Canada.

Furthermore, there are various centers set up to help report and respond to ransomware incidents, including the Canadian Anti-fraud Centre, which is Canada's central repository for information about fraud, including ransomware.

It also helps citizens and businesses with reporting, learning, recognizing, and protecting from fraud and works with law enforcement and governments within Canada to disrupt cyber crime.

The Canadian Centre for Cyber Security, as I mentioned, they're a premier authority on cyber security.

They are a single, unified source of expert advice, guidance, services and support on cybersecurity, and they lead the government's response to cyber security events.

We have, as well, the National Cyber Crime Coordination Unit, or the NC3 within the RCMP.

And they're responsible for coordinating cyber crime investigations in Canada, working with partners internationally to combat cyber crime and provide investigative advice and guidance to all levels of Canadian police.

Furthermore, the NC3 produces actionable cyber crime intelligence for Canadian police and is implementing a new cyber crime and fraud reporting system in partnership with the Canadian Anti-fraud Centre.

Governments, at all levels are interconnected and can become a target of a ransomware attack.

It's important that we work together to share information that helps detect, or better yet, prevent an attack, and share information about incidents that do happen to help with the response and prevent further spread.

Next slide please.

Thank you.

As I'd mentioned, here are some links that I encourage you to explore and share.

There are a lot of resources available to counter the ransomware threat.

And again, I'll emphasize that it's imperative we all work together to deter these actors from targeting Canadians and Canadian businesses by raising our defenses and stopping the payment of ransom fees.

Thank you for that, and I'll open it up for discussion.

Dafna: Thank you so much (INAUDIBLE) and much appreciated, as always, and a few questions for you.

It's always tough to tell the future, of course, especially as there is so much uncertainty in the world, particularly right now.

But let me ask you to make some predictions about (INAUDIBLE).

In your view, is the ransomware problem going to get worse before it gets better? Do you see technology solutions coming down the road that can help us solve the ransomware problem? Where do you see the future with ransomware?

Colleen: The future for ransomware, hard to say.

(INAUDIBLE) 19 weeks, the number of attacks decreased globally (INAUDIBLE).

So, in contrast in Canada, where the attacks have been increasing, it might be due to how digitized Canadians are and to our propensity to pay for unlocking these encrypted systems.

And the unfortunate truth is that cyber criminals are opportunistic, meaning that they take advantage of any situation they can in an effort to reach their financial goals.

And this has been the case during the current pandemic environment where businesses had to facilitate working from home for a lot of the workforce and cyber criminals were quick to use that urgency and uncertainty of the situation to facilitate their attacks.

So obviously, looking to the future, they're inevitably going to seek to exploit other similar opportunities.

And whether it's a second wave of the pandemic or another situation in the future, it's likely that we'll continue to see the trend of these increasingly targeted attacks and increasingly large ransom demands.

Regarding your question on the technology solutions.

At the end of the day, there's unfortunately, no one-size-fits all solution to ransomware, and I don't think that there ever will be.

But I don't wanna end on a down note either.

There are a lot of tools, advice and guidance that exist to help, not just individual Canadians, but organizations prevent an attack, such as the guidance that I mentioned that was developed by the Cyber Centre.

And as I mentioned just a bit ago, there are free decryption tools available and things that can assist victims in their recovery.

So, the recently released Canadian Shield that can help protect from attacks and things like artificial intelligence will also help in preventing some of these attacks.

Also, I have to say that the technology, techniques and processes that are being developed to defend against these threats, such as ransomware, they're evolving rapidly as well.

And I think the more that we're willing to embrace these preventative measures and new technologies to protect and recover, the better.

And I really wanna emphasize again, by all of us doing our parts together, we're that much stronger.

Dafna: Thank you for that.

Thank you for that, Colleen.

And just a couple of minutes left, but I did wanna pick up on one of the points that you made in your presentation regarding the tipping point at which ransomware becomes a national security concern.

Do you think that ransomware is a national security concern in Canada right now? Has it reached that tipping point in your view?

Colleen: Well, it became, I'll say c concern when it became an attractive tool for nation states, whether to make money or to masquerade information, stealing operations like financial crimes.

But I have to say, thankfully, ransomware attacks in Canada have not escalated to a level that qualifies as a national security emergency.

But at the global stage, what we're seeing is worrisome.

As I mentioned, we recently saw an instance where a ransomware attack caused Argentina to close immigration checkpoints for several hours.

An attack that interrupted a federal government's operations and the attacks are having a real (INAUDIBLE).

We need to be prepared from national security (INAUDIBLE) across Canada.

Dafna: Thank you.

And last question for you just about ransomware.

You talked about, and enumerated the very, very good reasons not to pay ransomware.

As you appreciate, as we can all acknowledge, it's a very tough situation, especially for smaller organizations that find themselves in that circumstance to make that judgment about ransomware.

Can you say just a little bit more about your point about not paying ransomware? 'Cause I think it's a really important one for people to take away.

Colleen: Yeah.

Well, in a very simplistic world or viewpoint, profit being what motivates the vast majority of ransomware attacks, if nobody pays, no ransomware.

So unfortunately, that's not the case.

You're absolutely correct.

When an organization or individuals hit by a ransomware attack and their data's held for ransom, they're in a really challenging position and they've got a lot of difficult decisions to make.

The process can be made easier by having the strong recovery procedures, a

continuity and disaster recovery plan.

But at the end of the day, there are a number of decisions that need to be taken and factors weighed, from costs, access to security (INAUDIBLE), urgency of the recovery.

Are there legal regulatory obligations? There are so many considerations that businesses have to take into account.

And unfortunately, malicious actors, they recognize these pressures on the victims and they know exactly what their payment capacity is.

They've become really adept at manipulating the victim by employing pressure tactics.

And ransom demands are often accompanied by threats to increase the ransom or delete decryption key, make a payment right away.

So, we're seeing a growing trend of data exfiltration and ransomware attacks with attackers publishing stolen data online if victims don't pay.

So, there's a lot of pressure to pay and restore the data, but we're still discouraging paying the ransom in these attacks for all of the reasons that we discussed.

Dafna: Colleen, thank you so much for your presentation.

This brings us to the end of our fourth session.

Thank you for sharing your expertise with us and thank you for this discussion.

Colleen: I'm happy to do it. Thanks for having me.

Dafna: Thanks so much, Colleen.

And as I said, that concludes our fourth session.

As before, when this session closes, all attendees will be sent back out to the lobby where you can network with others and follow the Twitter feeds.

Please click back into our fifth session at 12:30am sharp.

We will hear from Michele Mullen, who will talk to us about working with the Canadian Centre for Cyber Security.

You don't wanna miss that. See you all in a few minutes.