Cybersecurity and municipalities: The ransomware epidemic

David TS Fraser - david.fraser@mcinnescooper.com

NSFM Virtual Seminar 2021

Outline

- Baseline legal obligations of municipalities
- Additional considerations re critical infrastructure
- The ransomware epidemic
  - Evolution of ransomware
- Proactive risk mitigation and incident planning

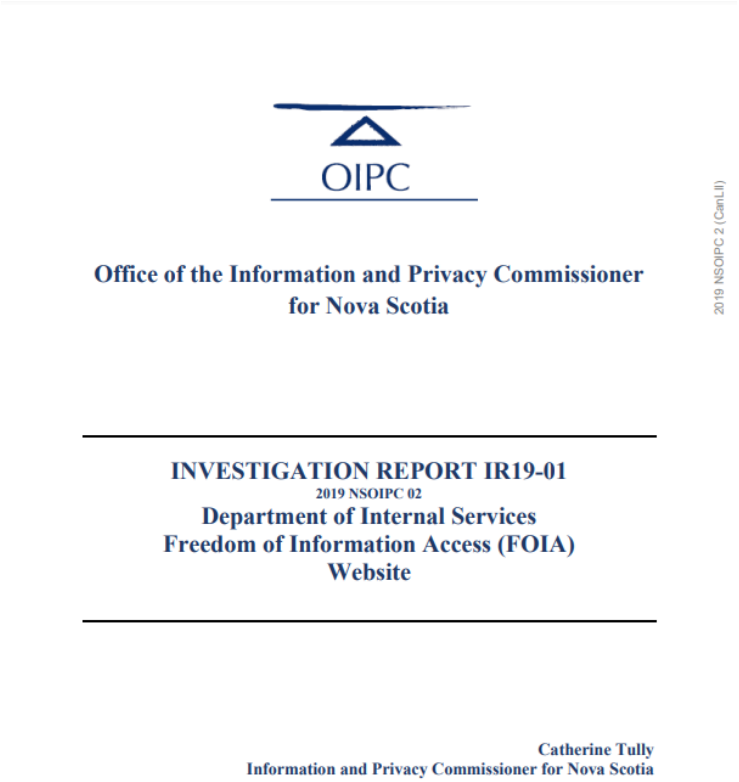
Legal obligations

- All municipalities in NS are subject to the *Municipal Government Act*, part XX of which largely mirrors the *Freedom of Information and Protection of Privacy Act*. These generally place obligations to protect *personal information*.

  "483(3) The responsible officer shall protect *personal information* by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal."

Adequacy of safeguards

1. Contextual
2. Sensitivity
3. Not technically prescriptive
4. Foreseeability
5. Trust
6. Industry standards
7. Cost
8. Life cycle
9. Format
10. Timing
11. Documentation



OIPC

Office of the Information and Privacy Commissioner
for Nova Scotia

2019 NSOIPC 2 (CanLII)

INVESTIGATION REPORT IR19-01
2019 NSOIPC 02
Department of Internal Services
Freedom of Information Access (FOIA)
Website

Catherine Tully
Information and Privacy Commissioner for Nova Scotia

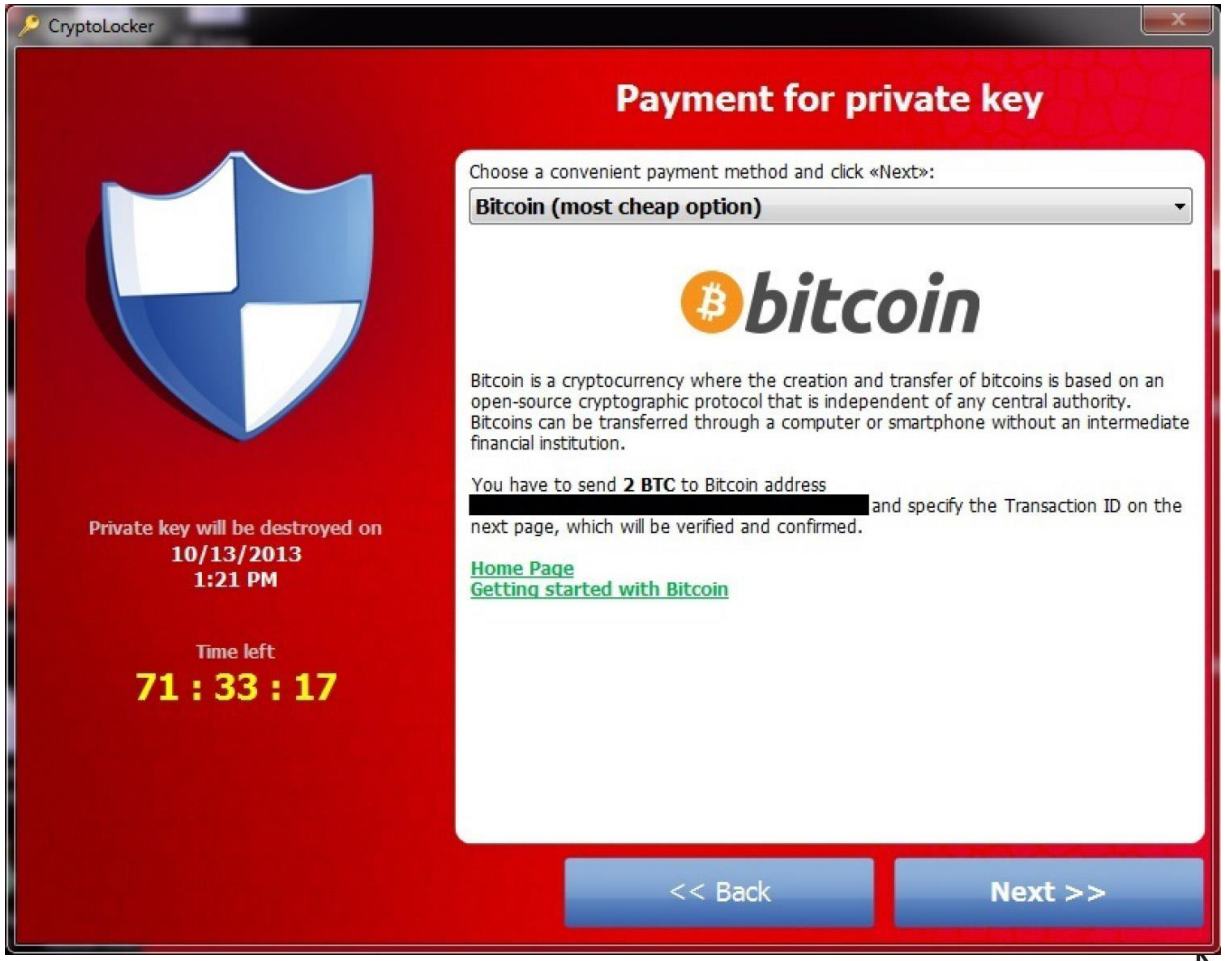
Legal obligations

- Part XX of the MGA likely does not oust the common law duty of care that may exist. We've seen an explosion of privacy-related class actions based on
  1. New privacy torts – intrusion upon seclusion and public disclosure of private facts
  2. Negligence – failure to meet the standard of care expected
  3. Breach of confidence
  4. Breach of contract

Critical infrastructure

- The risk to life and property is significantly increased for critical infrastructure managed by municipalities:
  - Water
  - Electric
  - Some roads, bridges
- Consequences of being forced offline can be enormous, even life or death.

Ransomware epidemic



History of ransomware

- First seen in 1989 targeting healthcare – the “AIDS Trojan”. Distributed by infected floppy disks.
- Early virus and malware was mainly destructive, but ransomware coupled with cryptocurrencies made it a very lucrative business.
- Before bitcoin, payments were made by cheque or corner-store money wiring services.

Ottawa

Ottawa Hospital targeted by cyberattack

Hackers target four computers but no data compromised, says hospital

The Canadian Press · Posted: Mar 13, 2016 9:26 AM ET | Last Updated: March 13, 2016

Victoria

This article is more than 3 years old

Traffic cameras in Victoria infected by WannaCry ransomware

State government says 55 cameras were affected after a contractor introduced the virus to the system by mistake

Naaman Zhou
@naamanzhou

Thu 22 Jun 2017 04.46 BST

▲ Speed cameras affected by the problem will be fixed in the 'next couple of days'. Photograph: Alan Porritt/AAP

Approximately 55 traffic cameras in Victoria have been infected with the WannaCry ransomware, according to the Victorian department of justice.

Intersection and highway cameras across the state have been affected by the malware, which caused chaos around the world by attacking the British National Health Service and other organisations in May.

METRO

NYC Law Department's network frozen after cyberattack

By Ben Feuerherd

June 7, 2021 | 3:11pm | Updated

Too close to home …

New Brunswick

Officials confirm cyberattack on Saint John was ransomware

No evidence that personal information was stolen, says city manager

Mia Urquhart · CBC News · Posted: Nov 17, 2020 5:13 PM AT | Last Updated: November 17, 2020

Saint John city manager John Collin confirmed at a news conference Tuesday afternoon that the city's recent attack was ransomware. (Roger Cosman/CBC)

POPULAR NOW IN NEWS

1 LIVE
Mandatory hotel stays, 14-day quarantine period coming to an end for fully vaccinated Canadians
3821 reading now

2 UPDATED
Manitoba to give nearly $2M in prizes to people who get vaccinated
1138 reading now

3 UPDATED
Peel's top doctor warns 'potential 4th wave' of COVID-19 brewing due to delta variant
949 reading now

4 When, where and how to see the June 10 annular solar eclipse
933 reading now

5 Rehiring is finally on the table for more restaurants — but not all workers are coming back
522 reading now

New Brunswick

Saint John will rebuild from scratch after cyberattack, cover costs from reserves

'Extensive' attack means rebuilding is better choice, city manager says

Hadeel Ibrahim · CBC News · Posted: Jan 12, 2021 7:37 AM AT | Last Updated: January 12

Saint John city manager John Collin said rebuilding the network could take four to six months, if not more. (Connell Smith, CBC file photo)

POPULAR NOW IN NEWS

1 LIVE
Mandatory hotel stays, 14-day quarantine period coming to an end for fully vaccinated Canadians
3821 reading now

2 UPDATED
Manitoba to give nearly $2M in prizes to people who get vaccinated
1138 reading now

3 UPDATED
Peel's top doctor warns 'potential 4th wave' of COVID-19 brewing due to delta variant
949 reading now

4 When, where and how to see the June 10 annular solar eclipse
933 reading now

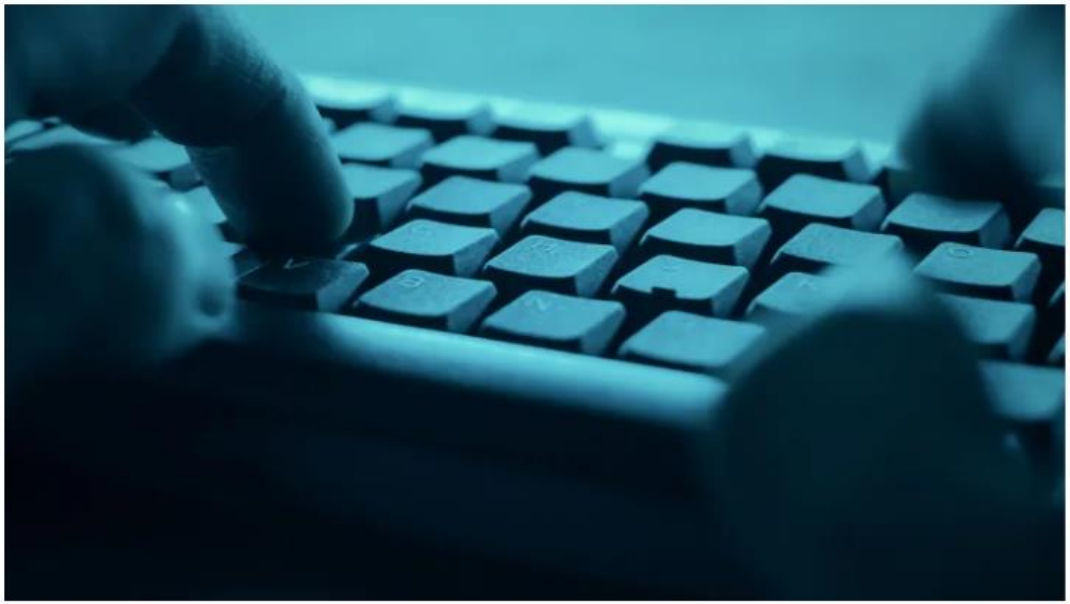
5 Rehiring is finally on the table for more restaurants — but not all workers are coming back
522 reading now

New Brunswick

$2.9M Saint John cyberattack bill to be mostly covered by insurance

City refused to pay hackers demand for between $17 and $20M to release information

Hadeel Ibrahim · CBC News · Posted: Apr 07, 2021 8:00 AM AT | Last Updated: April 7



Saint John was hit with a ransomware attack on Nov. 13, 2020. (PabloLagarto/Shutterstock)

POPULAR NOW IN NEWS

1 LIVE
Mandatory hotel stays, 14-day quarantine period coming to an end for fully vaccinated Canadians
3821 reading now

2 UPDATED
Manitoba to give nearly $2M in prizes to people who get vaccinated
1138 reading now

3 UPDATED
Peel's top doctor warns 'potential 4th wave' of COVID-19 brewing due to delta variant
949 reading now

4 When, where and how to see the June 10 annular solar eclipse
933 reading now

5 Rehiring is finally on the table for more restaurants — but not all workers are coming back
522 reading now

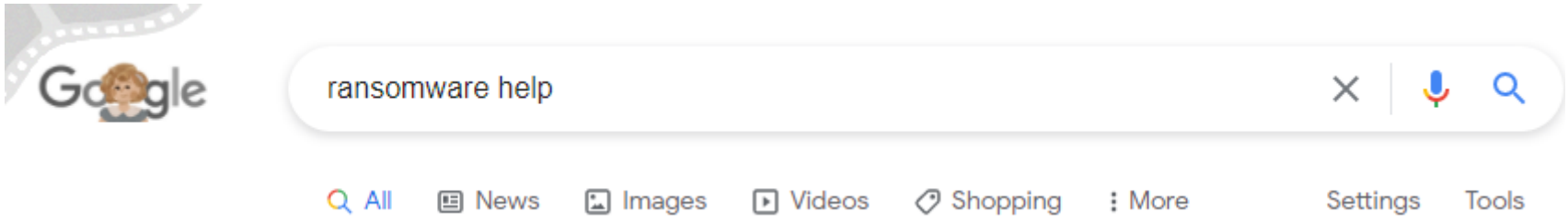
From ransom to extortion …

- As organizations have upped their readiness for ransomware, this has hit the bottom line for the bad guys.
- We're now more commonly seeing ransomware preceded by the plundering of systems and exfiltration of data.
- "If you don't pay up, we'll not give you the encryption keys and we'll post all your customer data on the dark web."

From ransom to extortion …

- If your data is just locked up, you at least know where it is.
- Exfiltration completely changes things. You have no idea if your data is out there and access to it is uncontrolled.

Preparedness and prevention



Not if, but when …

- Your networks are actively being targeted by automated, scalable attacks.
- Ask yourself, “are all of our doors locked?” Because someone is jiggling each knob 24/7.

Ask your IT folks …

- Backups are critical and make sure they are offline.
- Keep all systems patched
- Use antivirus and anti-spam solutions
- Disable macros and scripts
- Segment your networks
- Manage privileges
- Actively monitor what's going on with your networks **and through** your networks
- Log everything and retain your logs
- Block remote access from untrusted IP ranges

Secure users and endpoints

- Use multi-factor authentication
- Lock down remote access
- Social engineering and phishing training
- Screen all attachments and strip all scripts from incoming mail
- Limit personal use of work devices
- Limit use of USB storage devices
- Use mobile device management tools
- Patch all the things
- Have a reporting plan for anything sketchy

Be prepared

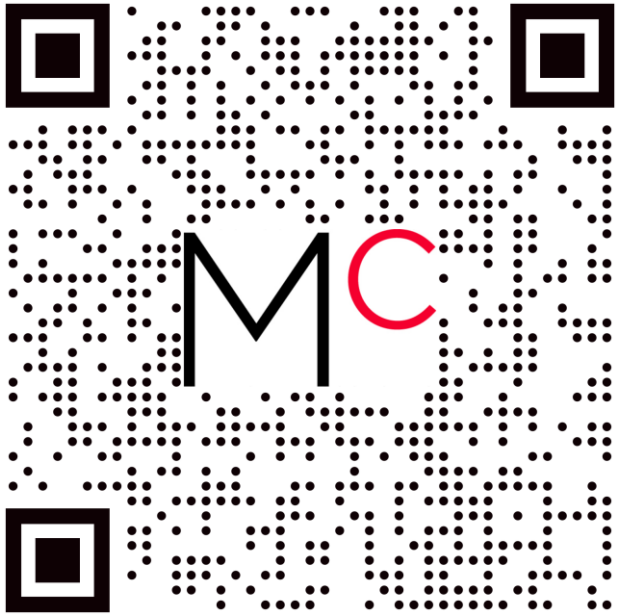
- Check your insurance – if you have coverage, your insurer can likely help develop and implement your plan
- Have your team and your plan in place before it happens
- Need to recognize and immediately escalate
- Your team should include
  - Senior decision-makers
  - Senior IT personnel
  - Communications personnel
  - Cybersecurity firm that is familiar with your systems
  - Internal and outside counsel
  - Risk management
  - Law enforcement liaison

Be prepared

- Regularly test your ability to **restore** from backups
- Carry out regular table-top exercises
- Have a way of contacting all your key personnel if all your systems are down or have been taken offline.
- Don’t expect much help from the police.


PRESS ANY KEY!

Questions?



Get Legal Alerts & Updates:

mcinnescooper.com/subscribe/

We work for the best: our clients.
mcinnescooper.com

MCINNES COOPER

Legal Notes

McInnes Cooper has prepared this document for information only; it is not intended to be legal advice. You should consult McInnes Cooper about your unique circumstances before acting on this information. McInnes Cooper excludes all liability for anything contained in this document and any use you make of it.

MCINNES COOPER

We work for the best: our clients.

mcinnescooper.com