# Ransomware Attack

Town of Midland

# Ransomware Attack – What Happened?

- Town IT personnel received an alert to unusual activity on the Town's email server in the early hours of Saturday, September 1
- By 10 a.m. Town IT staff had confirmed that we had been the victim of a cyber-attack, which infected the IT infrastructure with malware intended to encrypt files and systems
- We also received a ransom demand in exchange for a decryption key

# **Ransomware Attack – What Happened?** Cont'd

- On September 1, Administration contacted our insurance agent, AIG, who then connected the Town with a team of experts to assist in addressing this attack.
- On September 2, we were working with experts assisting with response, recovery and remediation, including forensic investigators, legal counsel and communications support

# **Ransomware Attack – What Happened?** Cont'd

- Through our AIG, we were connected with the following experts:
  - Fasken LLP – recognized leader in privacy and cybersecurity law.
  - Kivu Consulting – a leader in incident response and forensic investigations.
  - Edelman PR – Canadian leader in crisis management, consumer and corporate communications.

# Ransomware Attack – Impact

- We had no access to our servers/work email.
- Personal email or temporary email accounts were used so Administration could communicate with each other and the experts assisting our recovery efforts.
- Almost all Town services were impacted
- The Town's IP telephones, Interac payments, Marriage Licenses, Bus passes, Electronic Payments (some payments continued on tax and water account with reliance on paper notices)
- Processing of building permits were reverted to a manual exercise

# Ransomware Attack – Communications Strategy

- Developed an Incident Communications Strategy/Playbook
  - Objectives
  - Principles
  - Key Messages
  - Q&As
  - Media Release
  - Social Media statements
  - Internal speaking notes
  - Status updates

# Ransomware Attack – Communications Schedule

- Our goal was to be proactive with our communication.
- September 2/3 was spent preparing our playbook, including internal communication for staff and drafting our first media release.
- September 4 – CAO delivered an internal update to all staff at our various locations (Operations Centre, Water/Wastewater Plant, Town Hall) throughout the morning.
- Media release was distributed on the afternoon of September 4.

# Ransomware Attack – Factors

- Municipal government structure in a small municipality.
- 2018 Municipal Election campaign period was just ramping up.
- Canada Post Strike and Tax bills/bill payments
- Payroll

# Ransomware Attack – Election

- Top municipal election campaign discussion.
- Clashing views from different sides of the political/community spectrum.
- Candidates and residents questioning if the Town's IT infrastructure had heeded warnings on the need for warnings.

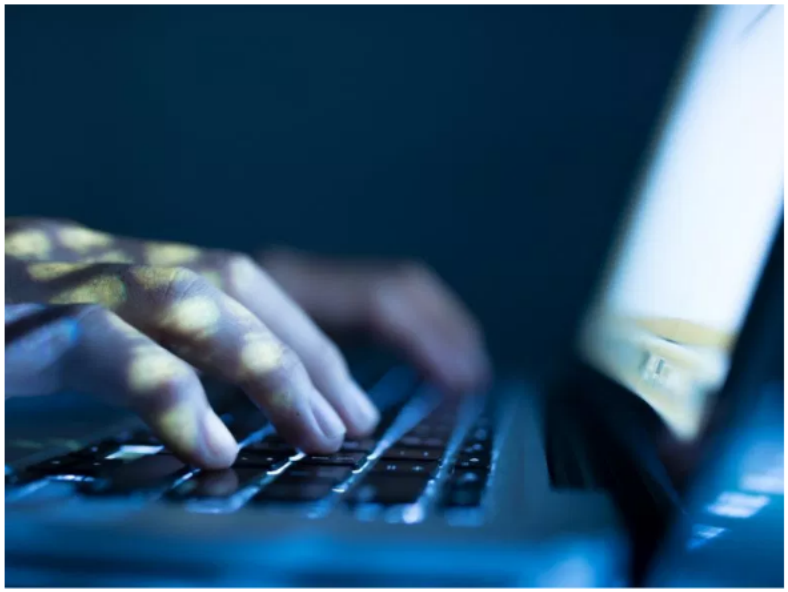
# Ransomware Attack – Media/Tone

- CTV Barrie did the first television report on the attack on September 5, interviewing our Mayor and CAO.
- Over the coming days the overall tone on social media and in traditional media shifted towards negative.
- On social media, Town's non-ransomware Facebook posts met with negative comments.

# Ransomware Attack – Shift in Tone

## 'Nobody likes having a shotgun pointed at their head': Cyber-thugs take aim at small town Ontario

*'Basically, these guys have these towns by the balls' — most small towns (and even large cities) don't have the budget to hire the best-of-the best IT workers*



Joe O'Connor

September 20, 2018
6:47 PM EDT

Last Updated
September 21, 2018
10:22 AM EDT

Filed under

Gord McKay was babysitting his granddaughters on the Saturday of the Labour Day long weekend, enjoying a little granddad-in-charge fun, when he received a panicked phone call. McKay is the mayor of Midland, Ont., a bustling tourist destination on the shores of Georgian Bay, about two hours north of Toronto. The call was from an employee with the town's IT department.

"The staff had come in early that day," the mayor recalled. "When they flipped on the computers they discovered most of them were inoperable because they

- On September 20, the National Post published an interview with our Mayor, that shifted the tone.
- Interview humanized the experience for our Mayor, and helped profile the Town's narrative and key messages on the attack.
- Positioned the Town as a potential champion for the importance of cyber security measures moving forward.

# Ransomware Attack – Recovery

- By September 24, all our services had been fully restored.
- That resulted in the ransomware talk dying down online and the media requests virtually stopped.
- In November 2018, a report was presented to Council outlining the details of the attack, including the ransom amount of 8 bitcoin.

# Ransomware Attack – Takeaways

- From a communications standpoint, timing is key!
- Be as transparent as possible, as soon as possible.
- Internal/external communications simultaneously to avoid pitfalls.
- Stay on course with your key messages and narrative.
- Everyone wants to know ‘How much?’ How will you handle this?
- Develop Q&A’s for your website, provide updates on the status of services.

# Ransomware Attack – Advice

- Prepare a crisis communications template/framework.
- Thank your IT Department!
- Funding proposal from your IT Department? Consider it favorably.
- Get insurance!
- Be honest.