Town of Midland

Ransomware Attack

Cyber Attack – When?

- 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

Insurance Support

- On Sept 1st Administration contacted our insurance agent, who indicated they would connect the Town with a team of experts to assist the Town in addressing this cyber security incident

- Sept 2nd we were working with a panel of experts engaged to assist with response, recovery and remediation, including forensic investigators, legal counsel and communications support

The Support Team

- *FASKEN (LLP)* - Fasken is a recognized leader in privacy and cybersecurity law with expertise in cybersecurity risk management, planning and incident response
- Their support team also included IT Experts with experience in dealing with ransomware situations and PR experts
- This support team was acquired through our insurers
- **Simcoe County** - IT Director & Staff were super-helpful throughout the process

Cyber Attack – What?

What was the nature of this attack?

- “Ransomware” attack
- The scope included Windows OS hosts that were online and was restricted to the town network. Other systems/PLCs such as network gear, printers, HVAC, etc. were unaffected
- The unauthorized actor executed Dharma ransomware on Server “X”. Backups were also encrypted. A credential harvesting tool was used
- SERVER “X”, the source of the attack, showed multiple Remote Desktop connections from foreign IP addresses
- During the compromise window, no data was accessed or exfiltrated by an unauthorized actor

Cyber Attack – Impacts?

What Services were impacted?

- Almost all 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

Unfolding of the event…

Snap-Shot of Day 1 (Saturday)

- IT Staff on site to commence disconnecting and securing servers in preparation of next steps
- Verify SCADA network (Water and Wastewater) not impacted by cyber attack and ensured connections to Town network severed.
- BFL Insurance Broker contacted and escalation of the cyber attack concerns to “on-call” Regional Manager and VP
- Confirmation of all Public access and Internet connections disconnected
- Mayor and Department Heads contacted to provide update on the status of the situation and set up conference call with department heads to determine next steps (Sunday)
- AIG – Insurance (Cyber Edge Claims Service) provided details of the incident – call was be set up AM next morning with the support team
- On the following days, OPP & IPC were formally informed as soon as possible