CASE STUDY

LOCAL GOVERNMENT

— INCIDENT – MALWARE

The client, a local government, experienced a large-scale malware attack. The malware caused serious disruption to critical services, including the municipalities' emergency responders. The disruption shut down hundreds of desktop computers as well as phones, emails and networks for several cities within the local government's charge.

— AXIS RESPONSE

The AXIS Incident Response Manager assembled a panel of cyber experts, working with the client to get a response plan in place and arranged the following assistance:

- IT professionals, to quickly restore the computer systems
- An incident response team, to guide the client through the process and address any legal implications of the attack

— OUTCOME

After a few weeks, the client's computer systems were restored. AXIS covered all expenses associated with the data recovery efforts.

The client was impressed with the speed and ability of the AXIS Incident Response Manager to provide the appropriate vendors to respond to the attack.

KEY CYBER COVERAGES TO CONSIDER

- Forensic and legal expense
- Data recovery expense
- Business interruption loss

PREPARE

- Prepare an Incident Response Plan and practice it regularly
- Provide cyber security and awareness training to all staff
- Keep the software and applications on servers and computers patched and updated
- Segment networks to hinder the spread of malicious software
- Apply multi-factor authentication (e.g. one-time token)
- Take steps to protect back-ups from ransomware