MUNICIPAL EXCESS LIABILITY JOINT INSURANCE FUND
9 Campus Drive, Suite 216
Parsippany, NJ 07054
Telephone (201) 881-7632

MEL CYBER TASK FORCE BULLETIN 18-01

Date: **April 12, 2018**

To: **Fund Commissioners of Member Joint Insurance Funds**

From: **Underwriting Manager, Conner Strong & Buckelew**

Re: **Preparedness is the key to managing Cybercrime! Do not let what happened in the City of Atlanta happen to you.**

On May 22nd, the City of Atlanta became encumbered by a Ransomware event, eventually found to be executed by the SamSam hacker group. Little information has been released to the public to date and the ransomware still persists, so it is difficult for us to understand what went wrong and how to better protect ourselves. However, the lack of information and ongoing event illustrates one of the most important lessons of cybersecurity:

PREPAREDNESS

Upon discovery of a cyber event, we know to immediately deploy the internal cyber response team and engage specialized cyber counsel. The triage executed by these teams primarily involves working through a decision tree of possibilities, such as:

1. **Action:** Pay the ransom now
    - **Benefit:** Gets systems back online (avoiding Business Interruption), helps avoid Public Relations issues and follow-on claims, helps eliminate potential losses from prolonged exposure and reduce the overall cost of the claim

2. **Action:** Do not pay ransom and engage forensics to clean system and engage backups
    - **Benefit:** Avoids ransom payment to criminals, reduces cost by just restoring backups

The success of these two options requires a good level of preparation before an incident occurs, most notably 1) an appropriate incident response plan, 2) establishing proper backup procedures and 3) identifying the risks and rewards of choosing different paths. The MEL Cyber Task Force includes all of these items, and much more, in the **MEL Cyber Risk Management Program**, in addition to template policy documents and specific steps to take to be prepared for a cyber event.

We will not know the full lessons learned until all details are disclosed, but below is a summary of details disclosed so far.

MEL Cyber Risk Management Program: https://njmel.org/wp-content/uploads/2017/12/Cyber-Risk-Management-Program.pdf

City of Atlanta Cyber Event, so far……

- Event reported on 3/22
  - Eventually identified as SamSam Ransomware by forensics firm
  - ~$51,000 ransom in bitcoin
  - ~6 million residents

- Certain cybersecurity warnings were made to the City at least 9 months prior
  - Mayor admitted not focusing on cybersecurity
  - Not up to date on security patches
  - Shows an insufficient backup policy

- Encryption by the ransomware spread across vast portions of the network
  - City cannot collect certain revenue streams, police efficiency is dropping, up to sixteen (16) years of data may be lost, no PII or PHI is known to be compromised, and access to online services is blocked
  - Shows lack of bifurcated network

What are your thoughts at this juncture, and how would you respond?

Even if your chosen remediation path failed, are you ready to endure over two weeks without your computer network?

cc: Fund Executive Directors
Fund Professionals
Risk Management Consultants