CARLTON FIELDS

Baltimore's Three-Week Ransomware Is a Warning for Other Local Governments to Prepare for Cyberattacks

CYBERSECURITY AND PRIVACY | PROPERTY & CASUALTY INSURANCE | MAY 31, 2019

Joseph W. Swanson

John E. Clabby

The Baltimore city government's email and other systems have been offline for more than three weeks as the result of a ransomware attack in early May. This is not the first local government to have been the victim of such malware, and it won't be the last.

These attacks can risk human life by hobbling first responders, including police, fire, and ambulance services. If nothing else, the financial cost of these attacks is staggering. An estimate released this week in the *Baltimore Sun* put the cost of the Baltimore incident at over $18 million. A similar attack on the city of Atlanta cost an estimated $17 million. These costs can stem from the investigation and response to the attack, as well as lost revenues where payment systems are offline.

Of course, these costs could be in addition to civil liability associated with the attack. That civil liability may be — but is not always — limited by sovereign immunity or statute. At a minimum, these attacks typically carry with them significant political fallout.

Local governments are favorite targets for cyberattackers, because those governments often do not have as robust cyber defenses as private organizations or are running outdated or unpatched operating systems and software. Further, local governments may not have adequate backup systems, which may compel them to pay the ransom.

Given all of this, city and other local governments, as well as administrative agencies, should take these steps to mitigate their risk and prepare for these attacks:

- Ensure that they have sufficient backups in place, that those backups are made regularly, and that the backups are "air gapped," or separated, from systems that can be infected with malware.
- Limit access to the organization's most sensitive networks to those employees who need that access to perform their job functions.
- Deploy strong email and systems passwords, changed often, with multifactor authentication for employees with more expansive system privileges.
- Draft and test an incident response plan that outlines roles and responsibilities in the event of a cyberattack.
- Work with risk managers and insurance brokers to determine whether they have sufficient coverage for cyberattacks and computer-based fraud.

Please contact Carlton Fields for more information on steps that you can take as a local government to protect yourself from ransomware and other cyberattacks.