FORTRESS

CYBERSECURITY SERVICES AND TOOLS

by Local Government Corporation

Cybersecurity Monitoring

Without a cybersecurity program, it is becoming extremely difficult for your office to protect against cyber-attacks, data breaches, or the theft of personal information. Cybercrimes are on the rise around the world and both personal identity and financial information theft continue to increase. It is critical to protect your office's data from attack – both internal and external.

LGC now offers Cyber security threat monitoring. Cyber monitoring provides real-time visibility of suspicious behavior or unauthorized system changes on your network. This puts you in the position of preventing such activity instead of just reacting to the all too real consequences.

The Growing Threat

- In 2020, at least 1,681 schools, colleges, universities as well as 113 federal, state, municipal governments and agencies were impacted by cybercriminals. The attacks on the education sector caused some schools to cancel both in-class and virtual classes and cost close to $2 million in ransom. The cost on the 113 government attacks is estimated to be near $915 million.

- Some of the most common targets of ransomware are municipal governments that are "under-resourced and under-managed" when it comes to cybersecurity, according to a cybersecurity expert from Dragos, Inc.
- Between May 2020 and May 2021, the FBI saw complaints about cyber-crime jump by 1 million.
- Notable incidents in 2020 included the attacks on the cities of Knoxville and Torrance, the Office of Court Administration of Texas, the Texas Department of Transportation and the 4th Judicial Court of Louisiana.

What does LGC do?

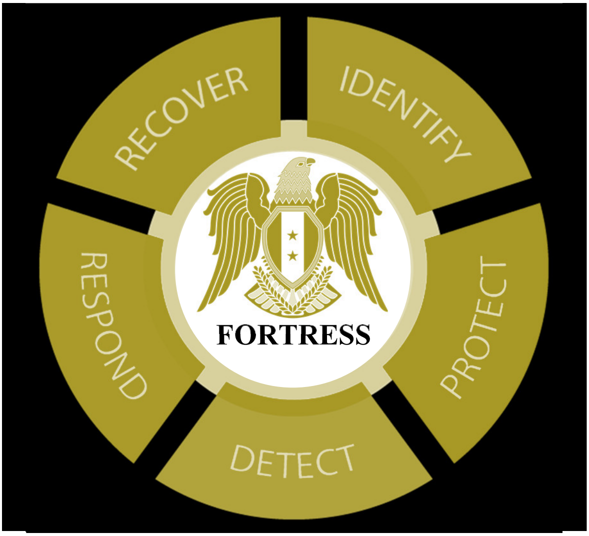
- LGC uses an advanced monitoring & detection software that helps identify a broad range of attacks. This will allow us to react in real time and notify you of attacks and assist in blocking those intrusions.
- Apply Operating Systems updates & other Microsoft product updates
- Apply SQL, Skype, & other program updates such as: Chrome, Firefox, & Adobe Reader
- LGC will monitor the behavior (processes in use, programs installed, and sites visited) of an endpoint (server & workstation)
- Realtime, behavior-based detection of malicious activity
- Notifies when the system is not performing as expected
- Notifies when hardware may be failing
- Isolation of a computer when a threat is detected
- Ransomware attack protection - detect an encryption event before it does damage
- Ransomware file restoration - restore files that have been encrypted
- LGC will assist you with audit or insurance questionnaires
- LGC will assist in system updates and maintain overall computer/system health.

<u>Your office should be aware and protected against</u>:

- ⇒ Malware
- ⇒ Ransomware
- ⇒ Spam & Phishing
- ⇒ Distributed denial of service (DDoS) attacks

What happens if my office has a cybersecurity breach?

- Although Fortress is another layer of security and allows us the ability to help monitor and assist you in your oversight, LGC cannot insure there will never be a vulnerability.



- If you do get infected, LGC will help assist you. This service is offered on a per office basis.

LOCAL GOVERNMENT CORPORATION
714 Armstrong Lane
Columbia, TN 38401
(800) 381-4540
marketing@localgovcorp.com