LOCAL GOVERNMENT CYBERSECURITY AND COVID-19

Laura Mateczun, J.D., Ph.D. Student | UMBC

Work from Home

The shift to telework as states issue stay at home and social distancing orders increases the opportunities for malicious actors to access government IT systems. Hundreds of thousands of government employees have made this shift. This strains computer networks and poses additional risks including the use of insecure WiFi networks, the use of personal devices when working with potentially sensitive information, and a surge in phishing emails.

Continuity of Operations Plans

A continuity of operations plan should be developed within your local government. Backing up your systems and data, in the event they are compromised, deleted or held for ransom is an important foundational step. Personally identifiable and other confidential information should always be encrypted. Without these plans essential government services can be interrupted or lost.

Cybersecurity Challenges

Cybersecurity is an essential government and private sector function. It plays a integral role in maintaining the critical infrastructure of the nation. This is especially true in times of disaster. The onset of the COVID-19 pandemic has raised cybersecurity issues to local governments in terms of an unprecedented shift of employees working remotely, an increase in agency website traffic of 100%, and an increase in attacks with a fourfold increase in cybersecurity complaints to the FBI, which all bring the potential for long term security risks.

In 2016, I along with a team of public policy, computer science and cybersecurity experts at the University of Maryland, Baltimore County conducted the first ever nationwide survey of local government cybersecurity. We found that local governments are under constant attack (47.1% at least daily), and that this important function is often poorly managed. Cybercriminals are using this pandemic as an opportunity to double down on their efforts, as seen in the increase in phishing attacks, and local governments must try to better address these threats.

Some of what your local government can do…

Actions / Policies:

- Follow best practices
- Use a safe videoconferencing tool
- Implement two factor authentication
- Back up and encrypt data
- Create incident response and continuity of operations plans
- Ensure adequate funding
- Establish a "culture of cybersecurity"

Resources:

- CISA telework best practices and video conferencing tips
- DHS guidance on essential critical infrastructure workers
- Check-lists and resources from the International City/County Management Association
- Webinars from the Public Technology Institute
- NICE Cybersecurity Workforce Framework Resource Center from NIST

The ensuing economic upheaval has caused further complication by creating budget shortfalls worse than the 2008 recession and the potential furloughing of thousands of local government employees. We found that the biggest barriers to administering adequate levels of cybersecurity mostly involve budgeting: 1) inability to pay competitive salaries, 2) insufficient number of staff, 3) lack of funds, 4) lack of adequately trained personnel, and 5) lack of end user accountability. Elected officials and managers need to become more aware of the importance of cybersecurity to the continuity of operations of their government, and actively support cybersecurity by maintaining it as an independent line item of more than ten percent of the budget.

A Culture of Cybersecurity Starts with You

Elected officials and employees at all levels must fully embrace and understand the importance of cybersecurity to their role in local government. This means practicing a culture of cyber awareness and hygiene according to publicly available best practices. Training key officials and staff is extremely useful, and periodic cybersecurity reminders to all employees is a relatively cost-friendly option. Holding all officials and employees accountable while also praising good behavior is key.