
# Audit Report
# Cybersecurity Awareness and Training
# December 7, 2018

**City Auditor's Office**
**Gregory L. McDowell, CPA, CIA**

# Audit Report
# Cybersecurity Awareness and Training
# December 7, 2018

## ***Purpose and Scope***

The purpose of this audit was to determine whether the City's Innovation and Technology Department (I&T) has established an effective cybersecurity awareness and training program. Cybersecurity is the overall system protecting an organization's computer hardware, software, and data from theft, damage, and disruption.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This report is intended for the use of the City Manager's Office, City Council, and I&T.

## ***Conclusion***

The risk of disruption to technology operations is high, as evidenced by the number of municipalities which have been attacked in the past year. I&T is taking appropriate action to further protect the City.

## ***Background***

With the increasing reliance upon the Internet and connected devices, cybersecurity represents a growing concern. Municipalities have become the target of "hackers" – those who attempt to infiltrate the organizations computer-supported systems. Attempts come in the form of "phishing" – a form of social engineering created to fraudulently convince a user to enter sensitive personal information, such as usernames, passwords, or credit card numbers. Phishing can be used to obtain access to nonpublic data and is subsequently used to deliver "malware" – malicious software that locks a user or entity's access to data until a ransom is paid (and therefore termed "ransomware").

The Department of Homeland Security's Multi-State Information Sharing and Analysis Center reported a 295% increase in total ransomware attacks on cities from 2014 to 2016.

In the last year, Mecklenburg County, NC (December 2017), Davidson County, NC (February 2018), and Atlanta, GA (March 2018) were victim to such attacks. Ransoms of $23,000 and $51,000 were demanded initially of Mecklenburg County and Atlanta. (The Davidson County ransom amount was undisclosed.)

Neither Atlanta nor Mecklenburg County paid their respective ransoms, however, costs incurred recovering from these attacks far exceeded the demands.

- The City of Atlanta reportedly suffered damages up to $17 million – the cost of reconstructing damaged or lost data, and subsequent actions taken to shore up security. In addition, the City experienced downtime due to employees being locked out of systems. More than a third of its software programs were partially or fully disabled. The Attorney's Office lost 71 of 77 computers and a decade of legal documents. Police dash cam footage was lost and could not be recovered.

- Initially, Mecklenburg County reported that property tax payments were hindered. Marriage applications could not be completed online. Code and Storm Water Services could not review plans or issue new permits. Applicants could not apply for vacant County positions. Polaris (real estate system) and the Department of Vital Records were down. Mecklenburg County Court's jury management system was disabled and its Department of Social Services was not able to process food stamp or Medicaid applications.

  More than 80 internal and public-facing online systems and services were restored in the month following the attack.

- Davidson County experienced a temporary shutdown of its Sheriff's Office and Tax Assessor's Office computers.

## ***Audit Finding and Recommendation***

### ***I&T should periodically evaluate the effectiveness of its cybersecurity awareness and training program.***

The weakest link in an organization's cybersecurity is often the users. According to local reporting, the attack on Mecklenburg County came after the County had invested $16 million over the three prior years to improve computer and network security. Davidson County reported that prior to its attack, every County employee already completed cyber training each year that teaches how to look for phishing emails.

A study of click rates on phishing tests[1] was conducted recently – that is, the rate that employees responded to phishing attempts by clicking on links provided via malicious emails. By industry, click rates ranged from 3% for the Defense Industrial Base to 16% for Telecommunications companies. The rate for Government was 13%, tied for third among the 17 identified industries.

The National Institute of Standards and Technology (NIST) publishes a Framework for Improving Critical Infrastructure Cybersecurity. The Framework consists of five functions, one of which is: "Protect – Develop and implement appropriate safeguards to ensure delivery of critical services" and includes a category titled "Awareness and Training."

[1] Wombat Security Technology's "State of the Phish" 2018 report

A critical step of any training and awareness program occurs *after* the program's implementation, and includes keeping the program up-to-date and monitoring its effectiveness. Such monitoring could include any combination of:

1. Identifying how useful participants found the training
2. Testing if participants improved their cybersecurity knowledge
3. Assessing the extent participants changed their behavior

The City's I&T Department has a cybersecurity awareness program in place as evident via the "Security Scoop" email newsletters, available training, brochures, and posters. However, there is no program in place to monitor the effectiveness of these activities.

A few years ago, I&T conducted a 100-user phishing test to assess employees' recognition of hacker activities. According to I&T, four employees failed the test by clicking the suspicious link; three of the four immediately notified I&T.

***Recommendation:*** I&T should periodically evaluate the effectiveness of its cybersecurity awareness and training program.

***I&T Response:*** I&T has purchased security awareness content. The program consists of modules that cover password security, phishing and malware. The modules include a learning portion, interactive enrichment, and required quizzes. The training will be mandatory for all employees with a City network account. The training was made available to IT Liaisons in November with expected rollout to all employees in 2019. I&T will periodically measure the effectiveness of the cybersecurity awareness and training program.