Audit Report

CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

T. Bert Fletcher, CPA, CGMA
City Auditor

Audit of Select City Cybersecurity Controls

Report #1718 ***September 15, 2017***

Preamble

We elected to issue a public report presenting at a summary level the results of our Audit of Select City Cybersecurity Controls. Details of certain aspects and characteristics of the City's information technology (IT) systems, for which disclosure may be in violation of Florida Statutes, Section 281.301 and good business practices, have intentionally not been included in this public report. To facilitate corrective measures and actions based on our audit, a separate report containing those details has been prepared and issued to appropriate City officials, management, and staff. That separate report is substantially exempt from disclosure under Florida Statutes, Section 119.071 and Section 281.301, as relating to or revealing security systems. Management has developed an action plan to address the issues and related recommendations in that confidential report. We will follow up and report to appropriate City officials and management on the efforts of applicable City staff in completing the established action plan steps as part of our periodic follow-up process.

Audit Purpose and Objectives

This audit was conducted for the purpose of evaluating the adequacy of cybersecurity controls established by the City to reasonably reduce the risk of data loss and corruption resulting from certain types of cyberattacks. Our specific audit objectives included the following:

- Determine if reasonable controls have been implemented to address the City's exposure to threats launched by malicious parties through the City's email system.
- Determine if the City is adequately managing and monitoring access to the City's network provided to third parties for the purpose of precluding those parties from unauthorized uses or manipulation of City data.
- Determine if reasonable controls have been implemented to address the City's exposure to threats launched through the City's primary website.

Audit Scope

Activity from 2012 through 2017 was analyzed in connection with certain audit procedures. However, our audit focused on controls in place during the time of our audit fieldwork, May 2017 through July 2017. Procedures performed to meet our audit objectives. included, but were not limited to:

- Interviewing City staff responsible for managing and monitoring cybersecurity risks and the controls established to address those risks.
- Developing and intentionally submitting a fictitious phishing email to City employees for the purpose of determining the City's susceptibility to employees improperly responding to such emails.
- Reviewing administrative access privileges granted to applicable City servers.

- Determining whether critical system patches and updates were applied to appropriate City servers in a timely manner.
- Determining if applicable server logs were being reviewed with appropriate action taken based on those reviews.
- Reviewing City network access permissions granted selected third parties and determining if those permissions were justified and properly managed, monitored, and controlled by applicable City staff.
- Identifying and evaluating methods used to protect the City's website.

We conducted this audit in accordance with the International Standards for the Professional Practice of Internal Auditing and Generally Accepted Government Auditing Standards. Those standards require 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

A cyberattack is defined as a deliberate exploitation of computer systems, technology-dependent enterprises, and networks. Cyberattacks use malicious code to alter computer code, logic, or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft. A cyberattack is also known as a computer network attack. The term "breach" is defined as the compromise of confidential or proprietary information maintained in electronic form as the result of a cyberattack.

Cyberattacks against major organizations have been widely publicized in recent years. Examples include both private entities, like Target in 2013, and governmental entities, such as the United States Office of Personnel Management (OPM) in 2015. Breaches resulting from cyberattacks result in loss or corruption of data and/or exposure of individuals to harm when personal and confidential data is compromised. The OPM cyberattack resulted in the theft of 21.5 million social security numbers. Furthermore, breaches are often costly to address and rectify and may harm the reputation of the compromised entity.

Costs to address breaches resulting from cyberattacks include financial resources and time and efforts of employees to identify the impacts (e.g., records compromised), notify those affected (e.g., employees or customers), cover any resulting losses, and determine the weaknesses within the entity's internal control structure that allowed the breach to occur. A 2016 Cost of Data Breach Study completed by the Ponemon Institute[1] reported the average total cost of a data breach in the United States is $7.01 million. The Ponemon study also reported the average cost per lost or stolen record containing sensitive or confidential information for government sector entities is $80. Further, International Business Machines Corporation (IBM) reported that, with a total of 39 documented breaches occurring in 2016, the government section was the second most attacked industry in 2016.

Types of Cyberattacks

Cyberattacks can be accomplished through various methods and mediums, including but not limited to, spam, and phishing. Successful attacks may result in the ability of a fraudulent entity to access (and potentially alter, delete, transfer, etc.) sensitive or confidential information. Such attacks are often accomplished through the installation of malware into an entity's systems and records. Malware is malicious software designed to damage or otherwise disrupt computer systems and the data therein. Malware includes computer viruses, worms, trojan horses, spyware, key loggers, and

[1] The Ponemon Institute, founded in 2002, is an independent research center dedicated to privacy, data protection, and information security policy.

ransomware. The following provides additional detail on the noted methods and mediums.

Spam: This is defined as irrelevant or unsolicited messages sent by email, typically to a large number of recipients for various purposes, such as advertisement of products or services. However, spam is also used for malicious purposes, to include enticing recipients to open hyperlinks that include malware.

Phishing: This is the fraudulent practice of sending emails purporting to be from reputable companies (entities) in order to induce individuals to reveal personal information, such as passwords and credit card numbers. If passwords are provided, the fraudulent party may then access and potentially alter, delete, remove, etc. sensitive or confidential information. Phishing typically involves the concept of "social engineering," whereby the fraudulent email is designed and structured in a manner that entices the recipient to click on a hyperlink (e.g., containing malware) or to provide sensitive or confidential information, such as login credentials/passwords, social security numbers, credit card numbers, and bank account numbers. For example, a phishing email directed to City employees could be structured to include the City's logo and names of City officials as an attempt to gain those employees' trust and encourage them to provide the requested information or click on a hyperlink that opens an inappropriate or harmful website.

Command Injection: This method involves a fraudulent entity planting (injecting) malicious programming code through a vulnerable software application. If the injection is successful, the fraudulent entity may gain access to sensitive and confidential information, install malware, delete or alter data, make data inaccessible to the owner entity, or deface the entity's website, including installing inappropriate data and information (pictures) onto the entity's website. Typically, the malicious code is injected through a form made available on an entity's website for the public (or customers) to provide feedback or transact business, that has fields without effective validation constraints. For example, forms made available through websites often requires the customer to enter a unique account number and address in specific fields within the form. If there are no validation controls that limit the specific character types and information that can be entered into those fields, a fraudulent entity could inject a malicious programming code into those fields that results in damage to the applicable entity's network and data.

Third Parties: In addition to being launched by malicious entities through emails (spam and phishing), cyberattacks can also be maliciously launched by or through third parties that are granted permissions to access an entity's network. Examples include vendors or contractors that need temporary access to an organization's network to perform their contracted responsibilities.

The Technology and Innovation Department (T&I) reported 3,651 email boxes were managed for City employees and departments at the time of our audit fieldwork (excluding the Consolidated Dispatch Agency which is not included in the scope of this audit). For the five-year period January 2012 through December 2016, an average of nearly 31,000 emails were processed daily by T&I, or an annual average of approximately 11,282,000 emails.

Audit Results

Because the continuing evolution of technology is coupled with ongoing advances in the sophistication of cyberattacks, it is difficult, if not impossible, for organizations to establish controls and safeguards that guarantee total protection of their data and networks from malicious acts. Nonetheless, because of the significant risk of data loss or corruption, organizations should enact appropriate, reasonable, and cost-beneficial measures for protection from such cyberattacks. In regard to the areas selected and reviewed, our audit showed that, overall, the City has reasonable and adequate cybersecurity measures in place to reduce the City's exposure to cyberattacks. However, areas were identified where enhancements to those measures should be made.

Acknowledgement

We would like to thank staff in the City's Technology and Innovation Department and in Communications for their cooperation and assistance during this audit.

Appointed Official's Response

City Manager:

One of our most important operational assets in the City of Tallahassee is our data. Threats to our data and data infrastructure must be taken seriously and all efforts to secure our data must be taken. This Audit demonstrates the importance the City of Tallahassee puts on providing best practices in data and network security. I want to thank the Audit team for the thorough dedication given to this audit. I would also like to thank the Technology and Innovation Department for the professional dedication given to meet these ever changing threats. Both teams play a vital role in providing the committed service the City of Tallahassee deserves.

Copies of this audit report #1718 may be obtained from the City Auditor's website (http://www.talgov.com/transparency/auditing-auditreports.aspx), by telephone (850 / 891-8397), by FAX (850 / 891-0912), by mail, or in person (City Auditor, 300 S. Adams Street, Mail Box A-22, Tallahassee, FL 32301-1731), or by e mail (auditors@talgov.com).

Audit conducted by:
Patrick A. Cowen, CPA, CISA, CIA, Senior IT Auditor
T. Bert Fletcher, CPA, CGMA, City Auditor