Office of the City Auditor

City of Gainesville, Florida

PUBLIC

Citywide Cybersecurity Audit- Phase II

September 6, 2022

Ginger Bigbie, CPA, CFE, City Auditor
200 E University Avenue, Room 211 Gainesville, FL 32601
352.334.5020

GAINESVILLE CITY COMMISSION

Lauren Poe, Mayor
David Arreola
Cynthia Chestnut
Desmon Duncan-Walker
Adrian Hayes-Santos
Reina Saco, Mayor-Commissioner Pro Tem
Harvey Ward

AUDIT COMMITTEE MEMBERS

Lauren Poe, Mayor
Reina Saco, Mayor-Commissioner Pro Tem
Harold Monk, CPA, CFE (Appointed)

TABLE OF CONTENTS

Citywide Cybersecurity Audit-Phase II

Executive Summary

What We Did

This information is not available in this public report, pursuant to Florida Statutes 119.0725(2)

Opportunities for Improvement

This information is not available in this public report, pursuant to Florida Statutes 119.0725(2)

We would like to thank Citywide Information Technology and security personnel, and police and fire rescue IT support staff, for their cooperation and professionalism throughout this audit.

INTRODUCTION

The objective of the Cybersecurity Phase II Audit was to provide an independent assessment of the City's cybersecurity governance structure, adequacy of current policies and procedures, and effectiveness of internal controls. *Background* information begins on page 5.

SCOPE AND METHODOLOGY

The scope of this review included an assessment of the design and operating effectiveness of controls related to the citywide cybersecurity program from January 1, 2022, through August 31, 2022.

The review was conducted through inquiry, observation, and limited testing for processes in scope. The Scope detail is not available in this public report, pursuant to Florida Statutes 119.0725(2).

RESULTS AND CONCLUSION

As a result of our review, we identified opportunities for improvement which are common across organizations of similar size and complexity. Audit issues and details are not available in this public report, pursuant to Florida Statutes 119.0725(2).

Local governments tend to operate under financial constraints that limit their ability to acquire and implement cybersecurity technology, as well as hire and retain cybersecurity staff. As local governments have learned the hard way, inadequate spending on cybersecurity often results in the predictable—breaches and the high cost associated with them. In the United States, two well-publicized cases of local government breaches—Atlanta, Georgia, in 2018, and Baltimore, Maryland, in 2019—cost those cities an estimated $12 million and $18 million.

We would like to thank citywide information technology and security personnel, and police and fire rescue IT support staff, for their cooperation and professionalism throughout this audit.

GOVERNMENT AUDITING STANDARDS COMPLIANCE

We conducted this audit engagement in accordance with *Generally Accepted Government Auditing Standards* and the *International Standards for the Professional Practice of Internal Auditing*. Those standards require that we plan and perform the engagement 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 observations and conclusions based on our audit objectives.

INTERNAL AUDIT TEAM

Ginger Bigbie, CPA, CFE, City Auditor
Briley Cordasco, CISA, Consultant (Lead Auditor for this engagement), Crowe LLP
Brecka Anderson, CIA, CFE, CGAP, Assistant City Auditor
Diana Ferguson-Satterthwaite, FCCA, CIA, Senior Internal Auditor
Peter DeMaris, Staff Auditor

BACKGROUND

The current threat landscape that organizations, including the City of Gainesville, are facing is rapidly changing as cyber-attacks evolve and become more sophisticated. This requires that organizations proactively identify, assess, and quantify known and emerging cybersecurity risks. Since the phase I cybersecurity assessment completed in 2020 by the City Auditor's Office, efforts have been made by the City to mature the cybersecurity program to protect against these threats and improve the City's cybersecurity posture.

As cyber-attacks targeting counties and municipalities continue to rise and new legislation is enforced, the City Auditor's Office conducted a phase II cybersecurity audit to continue assessing the City's cybersecurity readiness. The City Auditor's Office met with personnel in General Government Technology, Gainesville Regional Utilities (GRU) Information Technology, GRU Systems Control, Gainesville Police Department, and Gainesville Fire Rescue to understand the current state and direction of the City's cybersecurity program.

NIST Cybersecurity Framework

The city recently adopted the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) version 7.1 for its cybersecurity program, which integrates industry standards and best practices to manage cybersecurity risks. The Cybersecurity Architect is leading efforts to identify gaps that may exist and to provide recommendations on how to mitigate the risks associated with such gaps.

This 2022 phase II cybersecurity audit was modeled after the NIST Framework. The City Auditor's Office assessed the five key functions (Identify, Protect, Detect, Respond, and Recover) as referenced in Figure 1 below to address the risks of financial loss, negative publicity, harm to employees and neighbors, and the inability to deliver essential services due to:

- Malicious attempts to breach systems, networks, or personal computer devices.
- Inability to efficiently and timely detect, analyze, prioritize, report, and resolve security incidents.
- Inability to efficiently and timely recover from an event which may result in prolonged downtime, data loss, or additional recovery costs.

Figure 1 *– NIST Cybersecurity Framework*

We utilized the cybersecurity program maturity model in conjunction with the NIST framework functions to determine the maturity of the City's cybersecurity function. The City's maturity level may be credited to the collaboration of departments and combined experience of staff supporting the city's cybersecurity efforts.

Cybersecurity Regulatory Environment

Florida Statute 282.318 Cybersecurity, and **282.3185 Local Government Cybersecurity**, effective January 1, 2024, prohibits state agencies and local governments from paying ransomware demands. The law also requires annual employee cybersecurity training and other protective measures to secure its technology.

Section 3 of the local government statutes states that all local government employees with access to the local government's network must complete the basic cybersecurity training within 30 days after commencing employment and annually thereafter. It also mandates advanced cybersecurity training for technology professionals and employees with access to highly sensitive information within 30 days after employment and annually thereafter.

Section 4 of the local government statute requires adopting cybersecurity standards that safeguard its data, information technology, and resources to ensure availability, confidentiality, and integrity. In addition, the cybersecurity standards must be consistent with generally accepted best practices for cybersecurity, including the National Institute of Standards and Technology Cybersecurity Framework.

The Local Government Cybersecurity Act classifies five severity levels of cybersecurity incidents, with 5 being an emergency-level event and 1 being unlikely to impact public health and safety or governmental security. Local government entities must report all ransomware incidents and any cybersecurity incident determined by the local government to be of severity level 3, 4, or 5 to the proper authorities. These include the Cybersecurity Operations Center, the Cybercrime Office of the Department of Law Enforcement, and the sheriff who has jurisdiction over the local government as soon as possible but no later than 48 hours after the discovery of the cybersecurity incident and no later than 12 hours after the discovery of the ransomware incident.

Additionally, under section 6 of the statute, a local government must submit to the Florida Digital Service, within one week after the remediation of a cybersecurity incident or ransomware incident, an after-action report that summarizes the incident, the incident's resolution, and any insights gained as a result of the incident. By December 1, 2022, the Florida Digital Service shall establish guidelines and processes for submitting an after-action report.

The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) is a set of standards aimed at regulating, enforcing, monitoring and managing the security of the Bulk-Power System (BPS). The standards define the reliability requirements for planning and operating the North American BPS and are developed using a results-based approach that focuses on performance, risk management, and entity.

To further bolster cybersecurity defenses, the U.S. Department of Energy announced a $45 million grant to create, accelerate, and test technology that will protect our electric grid from cyber-attacks. Taking a proactive approach to evaluating and assessing the City's cybersecurity policies and procedures adds value by ensuring that current standards are in line with both present and future requirements, and also increases cybersecurity incident preparedness as a whole.

Current Events

The Colonial Pipeline hack that occurred in 2021 was the largest publicly disclosed cyber-attack against critical infrastructure in the U.S. After stealing data, the attackers infected the IT network with ransomware that affected many computer systems, including billing and accounting. Colonial Pipeline paid hackers $4.4 million to get the decryption key, enabling the company's IT staff to regain control of its systems. According to Crowdstrike's 2022 Global Threat Report, there was an 82% increase in ransomware-related data leaks in 2021. See Figure 3 on the next page.

In addition, attackers are increasingly attempting to accomplish their objectives without writing malware to the endpoint. Rather, they have been observed using legitimate credentials and built-in tools. See Figure 4 on the next page.

Figure 3 – Number of Ransomware-related Attacks Leading to Data Leaks, 2020 vs 2021

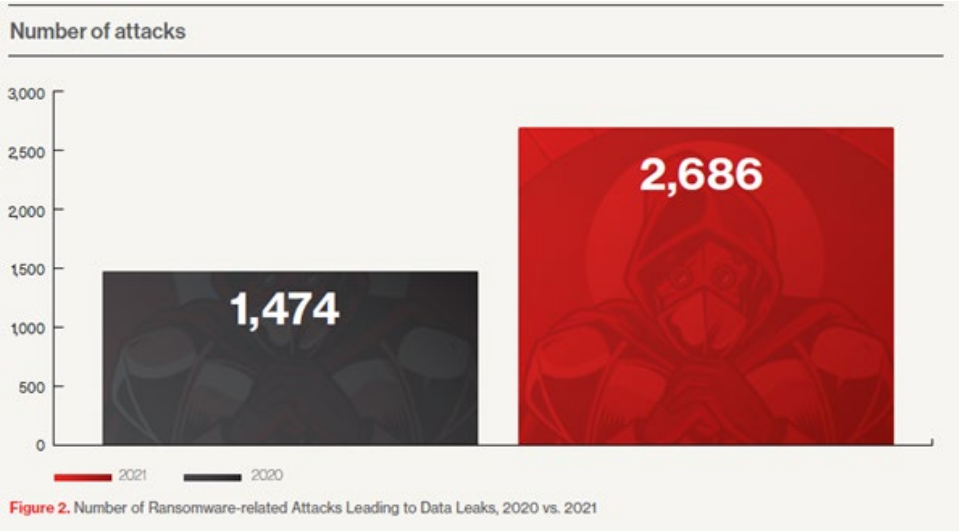
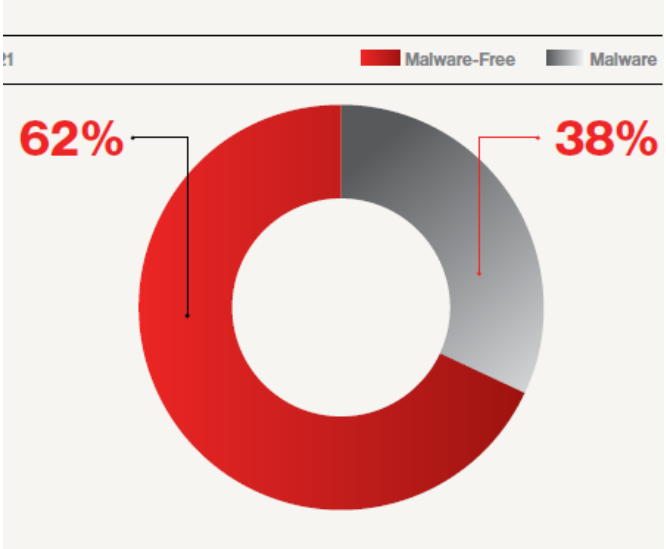


Figure 4 – Malware-free vs Malware



Source: CrowdStrike Security Cloud Q4 2021