Office of the City Auditor

City of Gainesville, Florida

Cybersecurity Readiness Review

September 23, 2020 **Report No. 2020-06**

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, Mayor-Commissioner Pro Tem *****
Adrian Hayes-Santos
Gail Johnson
Reina Saco
Gigi Simmons
Harvey Ward

***Audit & Finance Committee Member**

TABLE OF CONTENTS

INTRODUCTION 3
OBJECTIVES AND SCOPE 3
CONCLUSION 3
BACKGROUND 4
METHODOLOGY 4
RELATED FACTS AND FIGURES 5
GOVERNMENT AUDITING STANDARDS COMPLIANCE 7
INTERNAL AUDIT TEAM 7
APPENDIX 8

INTRODUCTION

The Cybersecurity Readiness Review was included in the City Auditor's 2020 Fiscal Year Audit Plan, Resolution # 190633, approved on December 5, 2019.

Multiple Florida local government organizations have been attacked by Ransomware in the last few years. As cyber-attacks targeting counties and municipalities are rising, the City Auditor's Office conducted a readiness review of the City's Cybersecurity governance and control environment.

According to the annually published Verizon Data Breach Incident Report, ransomware attacks accounted for only 4% of malware attacks in 2015. By 2018, ransomware attacks had risen to 50% and are reported at 61% of all malware attacks in the most recent 2020 report. In 2019, the U.S. was hit by an unprecedented and unrelenting barrage of ransomware attacks that impacted at least 966 government agencies, educational establishments, and healthcare providers at a potential cost in excess of $7.5 billion.

OBJECTIVES AND SCOPE

The objective of the review was to provide opportunity to improve the City's ability to identify, assess, and mitigate cybersecurity risks to an acceptable level. The scope included the current snapshot of information system data security controls for the period from January 1, 2020 to August 31, 2020.

The review was conducted through interviews, observations, and limited testing of control effectiveness in areas of higher risk, including the following processes critical to the City's cybersecurity readiness:

- Governance: strategic decision-making, objectives, policies and procedures which determine how the City detects, prevents, and responds to cyber events and incidents.
- Framework alignment: adoption of frameworks and guidelines that align with the City's goals and risk tolerance.
- Emerging risks: Identification of potential threats and vulnerabilities to ensure the confidentiality, integrity, and availability of the City's data.
- Staffing and funding resources: availability of resources to sufficiently mitigate cybersecurity risk to an acceptable level.

CONCLUSION

Our findings and recommendations, management action plans, and specific security features of the City's information systems are not included in this report. These nonpublic findings, recommendations, and management action plans were provided to the appropriate City leadership and are exempt from disclosure under Florida Statutes Section 119.071 and Section 281.301 as it relates to revealing security systems and issues. Remediation of findings will strengthen the City's overall cybersecurity program. These findings will be tracked as confidential but otherwise will be subject to the City Auditor audit issue follow up process.

BACKGROUND

Figure 1- NIST Cybersecurity Framework

Source: https://www.nist.gov/cyberframework

Although cybersecurity is ubiquitous within all areas of the City, this review was focused on IT areas of responsibility. Cyber-attacks exploit the increased complexity and connectivity of critical infrastructure systems, placing the City's security, economy, and public safety and health at risk. Similar to financial and reputational risks, cybersecurity risk affects the City's bottom line as it can drive up costs, affect revenue, and reduce the City's ability to innovate and serve its neighbors. Cybersecurity governance requires a very clear understanding of the City's overall strategic goals and objectives as well as cybersecurity risks. This ensures the ability Citywide to identify, protect, detect, respond, and recover from cybersecurity events.

This engagement focused on the City's IT cybersecurity governance controls of General Government (GG), Gainesville Regional Utilities (GRU), Traffic Operations, and Public Works' surveillance technology. The NIST Cybersecurity Framework version 1.1 illustrates five activities in the cybersecurity lifecycle: Identify, Protect, Detect, Respond, and Recover (see *Figure 1*). While there are several cybersecurity frameworks, including COBIT, NIST's Cybersecurity Framework is recognized globally for cybersecurity guidance and best practices. In addition to helping organizations manage and reduce risks, the NIST framework was designed to foster cybersecurity risk management and communications among both internal and external stakeholders.

METHODOLOGY

We utilized the COBIT 2019 Maturity Level for Focus Areas (see Appendix) to assess the City's cybersecurity readiness. Areas with a lower maturity level were determined to be less ready, whereas a higher score would indicate increased cybersecurity readiness. Additionally, maturity levels provide a standardized strategic objective when determining management's risk tolerance.

During this cybersecurity review, we interviewed key personnel and examined related policies and procedures. Areas of focus varied by each department's areas of responsibility. GG and GRU were reviewed for overall IT governance and security. Traffic Operations was reviewed for the City's security of traffic signal systems. Public Works was reviewed for the security of badge access systems and surveillance technology.

We reviewed information system security processes, procedures, and controls designed to identify, protect, detect, respond, and recover City data in the event of a cybersecurity incident. We assessed the control environment to determine whether the City:

- Adopted a Cybersecurity Governance Body and Framework

- Established, implemented, and communicated cybersecurity policies and procedures
- Retained IT Cybersecurity staff with adequate skills and training to effectively implement and manage a cybersecurity program
- Provided cybersecurity training to all City employees
- Implemented privacy controls that include the use of surveillance technology
- Assessed the privacy risk of third party applications prior to implementation
- Employed a data classification scheme
- Implemented a data retention policy
- Conducted business impact analyses that serve as the foundation for comprehensive business continuity plans.

RELATED FACTS AND FIGURES

Internal

Prior to fiscal year 2011, GG and GRU had separate IT functions. In 2011, the IT functions were consolidated in the areas of service desk, telecommunications, network services, and application support as per a memorandum of understanding (MOU), and the IT functions moved under the GRU General Manager for Utilities. In January 2016, the Chief Information Officer (CIO) was hired and implemented data security controls, set strategic IT initiatives, created the project management office to prioritize projects and the office of governance to establish compliance policies and procedures. In 2019, the CIO converted the 2011 MOU agreement to service level agreements that defined support, responsibilities, and expectations.

Efforts have enabled GRU to design processes, create policies, and build an IT staff with the necessary skill sets required for today's cybersecurity threats and challenges. IT personnel have obtained professional certifications such as Criminal Justice Information System (CJIS), Security Awareness Training, Cisco Certified Network Associate (CCNA), Information Systems Security Professional, CompTIA Security+, and Certified Information Systems Security Professional (CISSP), Project Manage Professional, CoBIT5 foundations, MS Azure foundations, ITIL foundations / practitioner, as well as multiple service desk certifications.

To reduce cybersecurity threats and increase security awareness, GRU began hosting citywide workshops under the brand name: "See Something, Say Something" and "Think before you click". As a result, on October 3, 2019, the City of Gainesville/Gainesville Regional Utilities was among 50 organizations honored by CSO (CSO50 a nationally recognized security organization), an online enterprise focused website that provides news, analysis and research on security and risk management. The annual award recognizes organizations for security projects and initiatives that demonstrate outstanding business value and thought leadership.

External

USD	BTC	Malware
$12.5M	~1,600	Ryuk
$10.9M	565	DoppelPaymer
$10.0M	1,326	REvil
$9.9M	1,250	Ryuk
$6.1M	850	Maze
$6.0M	763	REvil
$5.3M	680	Ryuk
$2.9M	375	DoppelPaymer
$2.5M	250	REvil
$2.5M	250	DoppelPaymer
$2.3M	300	Maze
$1.9M	250	DoppelPaymer
$1.6M	216	BitPaymer
$1.0M	128	Maze

Table 1.
Largest Ransom Demands Reported in 2019

Source: https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/

According to Crowdstrike's 2020 Global Threat Report, Ryuk (a type of crypto-ransomware) represented 38% of the largest ransom demands in 2019 (see *Figure 2*). Ryuk was also responsible for the attacks on Stuart and Key Biscayne.

Over the past two years, an additional six Florida municipalities have been victims of cyber-attacks, according to Naplesnews.com, including Collier County, City of Tallahassee, Riviera Beach, Lake City, Naples, and Pensacola.

A summary of these attacks are listed below.

In 2018 Collier County became a victim of a phishing scheme that netted attackers $184,000. In April 2019, the City of Tallahassee diverted almost half a million dollars out of their employee payroll from a cyber-attack of their human resources management application.

Sector	Known Ransomware	Details
Local Governments and Municipalities	RobbinHood, Ryuk, REvil, DoppelPaymer	The targeting of municipalities and local governments was popular among BGH criminal operators beginning in Spring 2019 and continuing through the rest of the year. Targets included several U.S. states and cities, and multiple incidents were seen in Spain.

Figure 3 – Commonly used Ransomware

Source: https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/

In April 2019, the City of Stuart was infected by the Ryuk computer virus, which forced them to disconnect from their service network. The virus originated from a desktop computer, which was likely infected when an employee was duped by a phishing email. Ryuk was also responsible for a cyber-attack in the town of Key Biscayne, in June 2019, from an infected email attachment.

The City of Riviera Beach paid 65 bitcoins, valued at about $600,000, after hackers ransomed the city's encrypted data in May 2019. Hackers accessed the City of Riviera Beach's computer network when an employee clicked a link in a phishing email, allowing malicious software to be installed.

In August 2019 the City of Naples fell victim to a sophisticated spear phishing cyber-attack that resulted in the loss of $700,000. In June 2019, a hacker targeted Lake City's computer systems, removed files, and issued a cryptocurrency ransom demand to restore those files. The ransom of 42 bitcoins was worth an estimated $480,000.

The Pensacola News Journal reported that the City of Pensacola suffered a cyber-attack in December 2019 that impacted phones, email, and various e-commerce services. After discovering the attack, the city disconnected its network from the Internet to minimize the damage. The city did not submit to the attackers' $1 million dollars demand and instead hired the global professional services company, Deloitte, for $140,000 to evaluate the extent of the cyber-attack.

GOVERNMENT AUDITING STANDARDS COMPLIANCE

We conducted this advisory engagement in conformance with the International Standards for the Professional Practice of Internal Auditing, and ISACA[1] IS Audit and Assurance Standards. 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
Eileen Marzak, CPA, CFE, Interim Assistant City Auditor
Vincent Iovino, CISA, CRISC, IT Audit Manager (Lead Auditor for this engagement)*
Brecka Anderson, CIA, CFE, CGAP, AICPA-COSO, Internal Audit Manager
Gregory Robeson, CPA, CIA, CFE, Senior Internal Auditor
Patrick Keegan, CISA, Senior IT Auditor*

**Denotes primary auditors on this engagement*

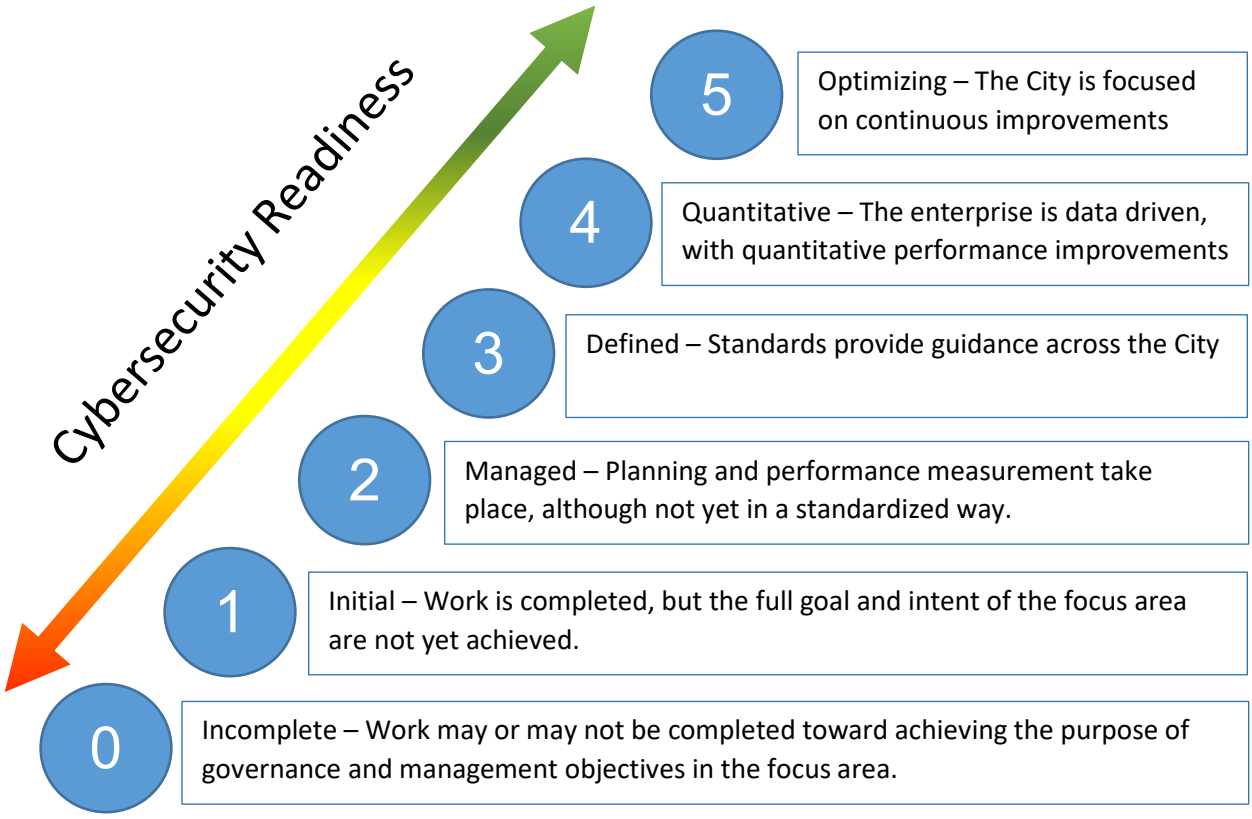
[1] Previously known as the Information Systems Audit and Control Association, ISACA is an independent, nonprofit, global association that engages in the development, adoption, and use of globally accepted industry-leading knowledge and practices for information systems.

APPENDIX

Maturity Levels for Focus Areas in Assessing Cybersecurity Readiness

The maturity model below is based on the COBIT 2019 *Focus Maturity Levels for Focus Areas* to assess the City's cybersecurity readiness in this review. Cybersecurity maturity reflects an organization's degree of preparedness to mitigate cyber threats and vulnerabilities. Cyber security is critical to every business and good security is strongly tied to business success and continuity.

In addition the maturity model provides a quantifiable measurement and guidance on how to reach the next level. The higher the maturity, the less chance that incidents or errors occur within implemented cybersecurity controls.



Source: COBIT 2019 Framework Introduction and Methodology Figure 6.3 on page 40.