Cape Coral
FLORIDA

CITY AUDITOR'S OFFICE

TO: Audit Committee

FROM: Timothy DiSano, Deputy City Auditor

DATE: July 08, 2022

SUBJECT: Cybersecurity

Background

At the May 11, 2022, Audit Committee Meeting, during the presentation of the City's Annual Comprehensive Audit Report (ACFR) the external auditors presented information about increasing cybersecurity risks in the world today. As part of the discussion, the question of how the City addresses these risks was discussed. In order to address these concerns and gather the information regarding the City's response to cybersecurity, the City Auditor's Office conducted a brief review of the policies and processes in place.

The Information Technology Services (ITS) Department consists of five divisions: Business Applications, Geographical Information Services, Information Technology and Communications, Network and Telecommunications, and Security.

The Security Division consists of 4 FTE's including, an IT Security Manager and three Network Security Administrators. Security staff work to ensure the confidentiality, integrity, and availability of information, data, systems, and operations. According to the ITS webpage, "The City has an information security program in place to ensure the confidentiality, integrity, and availability of information, data, systems, and operations. The security of City systems is architected in a manner that provides resilient, cost-effective, adequate controls while minimizing the effect on productivity."

Common cybersecurity threats or attacks facing the City today include ransomware; malware; social engineering attacks such as phishing; password attacks; Man-in-the-Middle attacks (MitM) whereby hackers place themselves between system users and the target server and intercept communication and sensitive information; and Distributed Denial of Service (DDoS), which can disrupt or stop functions and deny access.

These types of security attacks and breaches may result in loss of vital City systems which can cause business to stop, data loss or compromise, and loss of City funds. The impact of these breaches generally can be financial, legal, or reputational. Often breaches result in fines and fees; costly investigations; repairs to IT infrastructure; lawsuits associated with failure to protect customer data and privacy laws; and an overall loss of trust or diminished reputation with citizens.

Security Standards
Cybersecurity is generally described as the practice of protecting networks, devices and data from unauthorized access, disclosure, or criminal use by ensuring confidentiality, integrity, and availability of information. There are several industry regulations and cybersecurity standards available in the world today designed to help protect IT systems and its users.

Some common and well-known cybersecurity/security standards the City is currently following to reduce security risk include:

- **Center for Internet Security CIS standards (CIS)-** These are standards established by the Center for Internet Security which is a recognized organization in the security industry with over 20 years' experience. CIS established 18 critical security control categories, which include over 150 CIS critical security controls. In addition, they also provide potential specialized technology tools to help security practitioners implement and manage their cyber defenses. CIS has recently enhanced controls to version 8, to keep up with modern systems and software.

- **Payment Card Industry Data Security Standards (PCI DSS)-** These are security standards created in 2004 by the major credit card companies and are designed to ensure companies that accept, process or store credit card information, keep that information in an environment that is secure to protect cardholders against misuse of their personal information. Compliance is achieved by meeting a minimum set of requirements within 12 categories.

- **COBIT (Control Objectives for Information and Related Technology)-** This is a framework first released in 1996, COBIT are best practices in IT governance and management of an enterprise. COBIT is used in the development, implementation, monitoring and improvement of IT structures and provides globally accepted principles, tools to increase trust in and value from information systems.

Methodology and Procedures
The City Auditor's Office inquired with ITS about the current state of cybersecurity and specifically requested and reviewed information related to the following:

- Multi-year ITS Security Strategic Plan for FY22 to FY26
- IT Risk assessment performed for FY20 and FY21
- Penetration test assessment performed for FY20 to FY22
- Other assessments or reviews performed on various City IT infrastructure during FY21

We reviewed these documents to gain an understanding of the current status of ITS's efforts to minimize cybersecurity risk. The review was performed at the request of the Audit Committee to provide a response to concerns presented at the Audit Committee meeting. Work did not constitute an audit or non-audit service and therefore Generally Accepted Auditing Standards were not utilized or applied in this instance.

Status

To address cybersecurity threats or attacks and minimize risk of occurrence, best practices state that businesses should implement a comprehensive cybersecurity policy or plan, educate employees on cybersecurity threats, implement and test an incident response plan, keep software and systems up to date, sign up for alerts, and use strong passwords.

ITS has a strategic plan in place for FY22 through FY26. The plan includes security for the City, Charter School Authority (CSA), and Industrial Control Systems Networks. The plan discusses how the City can efficiently and effectively address the management, control, and protection of information technology assets. The plan was revised to incorporate updated CIS controls and to identify security outcomes and specific projects to bring the City, CSA, and Industrial Control Systems networks in line with the updated CIS security standards, as well as implementing additional controls Citywide.

ITS also deploys various products and tools to help mitigate overall ITS risk. These tools assist with prevention, detection, remediation, and response to security incidents in various areas. Some of these tools include anti-virus protection, patch management, and network monitoring. Additionally, ITS contracts with an external security firm that continuously monitors network traffic for deviations from the norm so malicious activity can be acted on as soon as possible. The firm also provides real-time security alerts as well as security incident response in the event of a breach.

ITS has also developed, and recently enhanced the City's ransomware attack response plan, by obtaining certain hardware and creating processes that will assist in the event of a ransomware attack. This response plan is periodically reviewed and tested for effectiveness. The department has also strengthened IT governance by developing comprehensive IT policies and procedures supporting (COBIT). These policies and procedures set IT standards and technical directives for four main domain areas including planning and organization, acquiring and implementation, delivering and support, and monitoring and evaluation. These policies are reviewed, updated, and approved at least every two years or as needed to reflect changes in the environment.

ITS holds bi-annual Steering Committee Meetings to provide strategic direction and updates on ITS related projects. These meetings are attended by department directors or their designees and various ITS personnel.

All City employees are required to take security awareness training and ITS uses best practice methods to access employee susceptibility to various email attacks. Employees are also required to change computer passwords frequently and ITS sets minimum passwords requirements based on industry standards.

In addition, various types of external and internal IT assessments are performed each year on a variety of IT assets. These assessments include internal, external, wireless, and web application penetration testing as well as an annual risk assessment. The results of these assessments are incorporated into the strategic plan to set a strategy for correcting areas of potential weaknesses, are discussed within the ITS Department staff at weekly meetings, and periodically with City management. The ITS Department's goal is to correct the high-risk areas identified as soon as possible, and medium risk areas as budgetary and staff availability permits.

Conclusion

Overall, based on our review of the documents provided and discussion with ITS staff, it appears ITS has a robust program in place to identify, address, and minimize cybersecurity risk to the City.

C: Mayor Gunter and Council Members
Rob Hernandez, City Manager
Connie Barron, Assistant City Manager
Michelle Hoffmann, ITS Director
Mark Mason, Financial Services Director
Kimberly Bruns, City Clerk
Dolores Menendez, City Attorney