City Auditor's Office

23-08 Information Technology Services-Information Technology Security Audit

Report Issued: September 29, 2023

Audit Report No. 23-08

Auditor-In-Charge: Timothy DiSano, CIA, CISA, CFE

P O Box 150027
815 Nicholas Pkwy.
Cape Coral, FL 33915-0027
Phone 239-242-3383 Fax 239-242-3384

TO: Mayor Gunter and Council Members

FROM: Andrea R. Russell, City Auditor

DATE: September 29, 2023

SUBJECT: Information Technology Services (ITS) – Information Technology (IT) Security Audit

The City Auditor's Office has completed the audit of the ITS Department IT Security. The audit was conducted in conformance with Generally Accepted Government Auditing Standards by the authority granted through City Ordinances 28-02 and 79-10.

We would like to express our sincere appreciation to the ITS Department management and staff for the courtesy, cooperation, and proactive attitude extended to the team members during the audit. If you have any questions or comments regarding this audit, please contact Andrea Russell at 242-3380 or Tim DiSano at 243-3308.

C: Michael Ilczyszyn, City Manager
Connie Barron, Assistant City Manager
Aleksandr Boksner, City Attorney
Kimberly Bruns, City Clerk
Michelle Hoffmann, ITS Director
Matthew Arsenault, ITS Security Manager
Audit Committee

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The City Auditor's Office conducted a performance audit of the ITS Department IT Security. This audit is included in the City Auditor's updated FY23 approved Audit Plan.

ITS has a robust process for ensuring important vulnerability patches are applied in a timely manner to help protect the City's IT infrastructure. Based on the test work performed and the audit recommendations noted, we concluded that although overall policies and procedures are in place to address IT security and provide an effective and timely response in the event of a cyberattack, policies and procedures for training, regulation compliance, and monitoring need improvement. For further details, see the Findings and Recommendations section. While we noted controls need improvement in these areas, we noted no material control deficiencies.

BACKGROUND

The City of Cape Coral and its residents depend on IT systems to deliver an array of critical daily functions such as public safety, financial services, and permit processing. The security of IT systems and related data supports the stability of city government operations and the safety and well-being of city residents. Disruption due to IT security incidents may be harmful to the City. Protecting these systems is important to maintaining public confidence in city government.

IT systems store and process large amounts of essential and confidential data. Residents, businesses, and employees are often required to share personal information with the City to participate in programs or receive services. In addition to the loss of public confidence, a data breach involving sensitive information can cause a government to face considerable tangible costs, including those associated with identifying and repairing damaged systems; notifying those effected; providing recovery and monitoring services to those affected; and paying fines.

There are many types of cyberattacks used by hackers including malware, denial-of-service, phishing and spoofing. One type of malware attack is ransomware, which encrypts an entity's data and devices and holds them hostage until a ransom is paid to restore access to files and networks. Typically, once the ransom is paid the victim receives a decryption key and can restore access. If the ransom payment is not paid, the attacker may publish the privileged information on Dark Web leak sites or block access to the files permanently. According to the State of Ransomware 2023 survey, the average ransom payment almost doubled from $812,380 in 2022 to $1,542,333 in 2023. According to the study, ransom amounts increased in 2022, with 40% reporting payments of $1 million or more, compared to only 11% in 2021.

It is important for entities to protect against cyberattacks to provide services and maintain and protect sensitive information. ITS Security is responsible for ensuring the security, integrity, and availability of all information, data, and systems for the City, and minimizing the effect of cyberattacks on productivity and the ability of the City to conduct business.

AUDIT OBJECTIVE

To determine if ITS policies, procedures, and incident response plans are sufficient to reduce the City's vulnerability, provide an effective timely response, and minimize damage to the City's IT infrastructure in the event of cyberattack.

STATEMENT OF AUDITING STANDARDS

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.

FINDINGS AND RECOMMENDATIONS

FINDING 2023-01: IT Security Training Compliance and Monitoring Needs Improvement
Rank: High

Condition:
City employees are required to complete basic cybersecurity training within 30 days of commencing employment and annually thereafter. In addition, Florida State Statute (FSS) 282.3185, effective 7/1/2022, requires certain employees with access to highly sensitive information to complete advanced cybersecurity training within 30 days of commencing employment[1] and annually thereafter. The City uses a training software program to track training including the cybersecurity training. ITS requires annual training be completed by August 31st each year. System access is revoked if employees do not complete the training. ITS communicates a list of individuals who have not completed the training to Department Directors every August. Human Resources (HR) provides updates on training upon request.

There is no monitoring or tracking outside of Microsoft Active Directory, which is continuously updated as staff are hired, leave City service, or promoted to a position requiring system access. There is no way to obtain historical data to monitor compliance due to the use of Active Directory, which is constantly updated. There is also no policy to identify positions with access to sensitive information, such as those in Financial Services or ITS, that would require advanced cybersecurity training. Because the requirements for training have not been formally communicated, HR informed us they receive emails from employees questioning why they are enrolled in the training, stating they do not access such information, and request to be removed from the training list. Administrative Regulation (AR) 72, Information Security Awareness Program, which discusses annual security awareness and training for all employees accessing City systems, including annual, new hire, and Payment Card Industry (PCI) parts 1 and 2 compliance training, has not been updated since 10/14/2016. New requirements became effective more than a year ago.[2]

We reviewed employee cybersecurity training records for FY22 and FY23 through 8/31/2023 to determine if employees received the appropriate training in accordance with the FSS. We noted the following results:

- New hire training
    - FY22, 37 of 48 (77%) new employees, hired after July 1, 2022, did not complete cybersecurity training within 30 days of commencing employment.
    - FY23, 20 of 27 (74%) new employees did not complete cybersecurity training within 30 days of commencing employment.
- Annual employee training[3]

[1] Training is also required for contract employees, as well as those who promote into a position that requires system access or access to sensitive information.
[2] See Finding 2023-02.
[3] Exception rate for FY22 was below reportable levels according to City Auditor's Office policy.

- FY23, four of 55 (7%) employees did not complete annual cybersecurity training.

- Highly sensitive (advanced) training completion[4]
  - FY23 Sensitive Information Training required for certain employees.
    - Five of 19 (26%) employees did not complete sensitive training.

  - FY23 IT Business Apps and IT Privilege Training required (for ITS employees only)
    - Three of seven (43%) employees IT Business App training not completed.
    - Two of 16 (13%) employees IT Privilege user training not completed.

  - FY23 PCI part 1 and PCI part 2 training
    - 55 of 93 (59%) employees PCI1 training not completed.
    - 56 of 91 (62%) employees PCI2 training not completed.

Criteria:
- FSS 282.3185
- AR 72
- City AR 0 AR Procedures

Cause:
- AR 72 is not updated for new FSS requirements
- No policy to identify which employees require advanced cybersecurity awareness training
- Insufficient monitoring of training requirements

Effect:
- Noncompliance with FSS 282.3185
- Increased risk for cybersecurity incidents, security breach
- Potential improper handling sensitive credit card information/PCI data

RECOMMENDATIONS:
2023-01a: Formalize the cybersecurity training program and monitor compliance for all employees.

2023-01b: Review and update AR 72, Information Security Awareness, in accordance with City policy for administrative regulations to ensure compliance with new IT requirements and regulations.

[4] Information for FY22 was not provided for testing.

Management Response and Corrective Action Plan:

2023-01a Select one of these boxes: ☒ **Agree** ☐ **Partially agree*** ☐ **Disagree***
***For partially agree or disagree a reason must be provided as part of your response:**

2023-01a *IT Security Training will be conducted using the security vendor's software. A similar process is in use today at the Charter Schools. The process is fully automated and provides managers real-time notifications when an employee is near their training deadline.*

IT will work with HR to automate the identification of employees requiring PCI training.

The anticipated completion date of this action plan reflects the impact of the City replacing the HR/Payroll system on 1/1/2024, and the additional time needed to complete the automations with the new system.

2023-01a Management Action Plan Coordinator: *ITS Director*
2023-01a Anticipated Completion Date: 04/01/2024

2023-01b Select one of these boxes: ☒ **Agree** ☐ **Partially agree*** ☐ **Disagree***
***For partially agree or disagree a reason must be provided as part of your response:**

2023-01b *IT will review and update AR 72 to reflect the Florida State Statute that governs the IT Security training.*

2023-01b Management Action Plan Coordinator: *ITS Director*
2023-01b Anticipated Completion Date: 04/01/2024

FINDING 2023-02: IT Regulation Monitoring and Compliance
Rank: High

Condition:
FSS 119.0725- Agency cybersecurity information; public records exemption; public meeting exemption, was enacted on 7/1/2022 and applies to information held by the City "before, on, or after" 7/1/2022. This statute precludes certain technology information from being stated in public documents such as reports or memos. The statute also includes an exemption from the Sunshine Law for portions of meetings that would reveal confidential or exempt IT security information, such as meeting agenda items and procurement documents. ITS did not formally communicate the details of the new legislation requirements in a timely manner to City employees impacted by the legislation. On 7/19/2023, a year after the legislation was enacted, ITS e-mailed certain employees informing them of the new FSS requirements. At the time of the audit, ITS has provided limited guidance explaining measures the City has in place, or will

put in place, to ensure compliance with the FSS and appropriately protect sensitive IT information. The City has not complied with this FSS.

The City currently uses various means to identify legislative updates that will affect the City, including an internal legislative liaison and external legislative law firm. The liaison monitors legislation and provides reports for the entire City. ITS does not utilize any means independent of the City-wide monitoring to stay informed of new legislation or changes to existing ones that impact IT. The current process did not allow for timely updates on this IT specific legislation.

Criteria:

- FSS 119.0725
- Florida League of Cities (FLC) 2022 Legislative Session Final Report dated 6/29/2022.

Cause:

- Insufficient ITS monitoring for new information technology statutory regulations.

Effect:

- Noncompliance with FSS 119.0725
- Potential release or exposure of confidential ITS information

RECOMMENDATION:

2023-02: Develop and document a process to monitor legislation and industry guidance specific to information technology.

Management Response and Corrective Action Plan:

2023-02 Select one of these boxes: ☒ **Agree** ☐ **Partially agree*** ☐ **Disagree***

***For partially agree or disagree a reason must be provided as part of your response:**

2023-02 *The IT Director is responsible for monitoring Federal, State and Local laws that impact the information technology operations for the City and for communicating those changes to other impacted departments. While this piece of legislation was an anomaly, we will modify our monitoring process. In addition to attending industry related webinars and conferences, the IT director will set a quarterly reminder to search for pending changes to laws that effect IT.*

2023-02 **Management Action Plan Coordinator:** *ITS Director*

2023-02 **Anticipated Completion Date:** 10/02/2023

SCOPE AND METHODOLOGY

Based on the work performed during the planning and the assessment of risk, the audit covers ITS security processes in place for the period of FY22 to FY23 through July 31, 2023. Testing was performed using applicable FSS, City Administrative Regulations, ITS Policies and Procedures Manual, and Incident Response Plans that were in place and applicable during the audit scope[5].

To achieve our audit objective, we conducted interviews and walkthroughs with key staff to gain an understanding of the security process, training, and incident response plans and reviewed applicable policies and procedures and relevant state statutes. Sample size and selection are based on the CAO approved sample methodology. We used judgmental and random sampling to select our samples.

We tested employee cybersecurity training requirements to verify compliance with applicable policies and regulations for required new hire, annual, and advanced training. We also tested a sample of vulnerability patches applied during the scope period to determine if the City has an appropriate process in place. Finally, we reviewed the ITS Department's incident response plan to ensure the plan is up to date, and if ITS staff receive the necessary training to provide a timely incident response in the event of a cyberattack. We evaluated the processes in place to ensure compliance with applicable regulations.

To achieve the audit objective, we evaluated and relied on information from the City's vulnerability management system and training tracking system. We initially deemed data reliable for testing our audit objective during planning; however, as a result of our fieldwork testing, we identified training requirement data compilation and monitoring need improvement.[6]

Unless specifically stated otherwise, based on our selection methods, and testing of transactions and records, we believe that it is reasonable to project our results to the population and ultimately draw our conclusions for testing, findings, and recommendations on those results. Additionally, for proper context, we have presented information concerning the value and/or size of the items selected for testing compared to the overall population and the value and/or size of the exceptions found in comparison to the items selected for testing.

[5] The scope for testing employee training compliance was extended to 8/31/2023 because historical training results are maintained only on an annual basis ending on 8/31. Information was available as of the training deadline of 8/31/2023. Testing as of the scope period 7/31/2023 would provide incomplete results. The extension only applies to this testing.

[6] See finding 2023-01 Security Training and Compliance and Monitoring Needs Improvement

APPENDIX A

Finding Classification
Findings are grouped into one of three classifications: High, Medium or Low. Those findings that are categorized as low are not included in the report but rather are communicated separately to management. Classifications prioritize the findings for management to address and also indicate the level of testing required to determine if a finding's Corrective Action Plan is fully implemented in accordance with recommendations and Management's Response.

High: A finding that is ranked as "High" will have a significant impact on the organization. It is one that *prevents* the achievement of a substantial part of significant goals or objectives, or noncompliance with federal, state or local laws, regulations, statutes or ordinances. Any exposure to loss or financial impact for a High finding is considered *material*. Examples include direct violation of City or Department policy, blatant deviation from established policy and procedure, such as actions taken to circumvent controls in place, material non-compliance with federal, state or local laws, regulations, statutes or ordinances, or an area where significant cost savings could be realized by the Department or the City through more efficient operations.

High findings require immediate management attention and should take management's priority when considering implementation for corrective action.

Medium: A "Medium" finding is one that *hinders* the accomplishment of a significant goal or objective or non-compliance with federal, state or local laws, regulations, statutes or ordinances, but can't be considered as preventing the accomplishment of the goal or objective or compliance with federal, state or local laws, regulations, statutes or ordinances. Exposure to loss or potential or actual financial impact is *significant but not material* to the Department or City. Examples include lack of monitoring of certain reports, insufficient policies and procedures, procedure in place or lack of procedure that can result in *potential* noncompliance with laws and or regulations.

Medium findings require management attention within a time frame that is agreed upon by the Department and the City Auditor. Priority for implementation of management's corrective action should be considered in light of other High or Low findings.

Low: A "Low" finding is one that warrants communication to management but is one that isn't considered as hindering the accomplishment of a significant goal or objective and isn't causing noncompliance with federal, state or local laws, regulations, statutes or ordinances. Financial impact or risk of loss is minimal to none; however, low findings can *hinder the effectiveness or quality of department operations and thus are communicated to management separately. Low ranked findings are not included in the final audit report.*

The City Auditor's Office will not follow up on the status of Low findings communicated to Management.