City Auditor's Office
Cybersecurity Audit

March 2021

City Auditor, Lori Brooks Jaquess, CPA, CIA, CGAP, CRMA
Assistant City Auditor, Susan Edwards, CIA, CFE
IT Auditor, Roshan Jayawardene, CISA

NOTE: This version of the Cybersecurity Audit Report has been redacted by the City Attorney's Office to remove confidential information that, if publicly released, could compromise the security of City assets.

City Auditor's Office

March 19, 2021

Honorable Mayor and Members of the City Council:

The City Auditor's Office has completed the Cybersecurity Audit. The purpose of the audit was to review and evaluate the City's current preparedness efforts related to cyber risks.

Management's response to our audit findings and recommendations, as well as target implementation dates and responsibility, is included following the report.

We would like to thank staff from the City's Information Technology Department for their full cooperation and assistance during the audit.

Lori Brooks Jaquess

Lori Brooks Jaquess, CPA, CIA, CGAP, CRMA
City Auditor

Attachment

cc: Trey Yelverton, City Manager
Jim Parajon, Deputy City Manager
Gilbert Perales, Deputy City Manager
Jennifer Wichmann, Assistant City Manager
Enrique Martinez, Chief Technology Officer
Yoko Matsumoto, Human Resources Director

Table of Contents

Executive Summary

The City Auditor's Office has completed the Cybersecurity Audit. 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 objective. The audit objective was to review and evaluate the City's current preparedness efforts related to cyber risks.

The City Auditor's Office noted strengths in the Information Technology (IT) department related to the following:

- [redacted]

We noted potential opportunities for improvement in the following areas:

- [redacted]

Details of audit findings, conclusions and recommendations are included in the following report.

Audit Scope and Methodology

The objective of the audit was to review and evaluate the City's current preparedness efforts related to cyber risks. The audit included a review of cybersecurity efforts between 2011 and 2020. To adequately address the audit objective and to describe the scope of work on internal controls, the following methodology was used in completing the audit:

- Interviewed staff and management in the IT department
- Reviewed contracts and deliverables applicable to software and third-party vendors
- Conducted research applicable to cybersecurity and security standards
- Examined remedial activity by IT staff
- Reviewed the phishing education program and test data
- Computed cost vs benefits applicable to third-party party security contractor

The audit was conducted in accordance with generally accepted government auditing standards. These standards require that we determine whether internal controls are significant to the audit objective. If internal controls are significant to the audit objective, the standards require that the auditor obtain an understanding of the controls. In understanding and evaluating internal controls, the City Auditor's Office adheres to the Committee of Sponsoring Organizations of the Treadway Commission's Internal Control – Integrated Framework (COSO Framework) as included in Standards for Internal Control in the Federal Government (Green Book).

According to the COSO Framework, internal control is a process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved. These objectives and related risks can be broadly classified into one or more of the following three categories: (1) Operations - effectiveness and efficiency of operations; (2) Reporting - reliability of reporting for internal and external use; and (3) Compliance - compliance with applicable laws and regulations.

In planning and performing the audit, we obtained an understanding of the cybersecurity efforts by the IT Department, including tasks performed by vendors and associated internal controls, and we assessed the internal control risks significant to our audit objective. We determined the following internal control components were significant to our audit objective:

- Control Environment - The IT security infrastructure and data assets under the control of the City's Information Technology Department
- Risk Assessment - Continuous assessment of security risks and cyber threat assessment to the City's technology infrastructure
- Control Activities - Threat mitigation and corrective action by IT staff relative to network perimeter security, initiated vulnerability assessments, and third-party vendor assessments
- Monitoring - Continuous monitoring of threats to the City's technology infrastructure per NIST cybersecurity guidelines
- Information and Communication - Updates and security briefings to keep staff and management informed of breaches, threat environment, and corrective action

The deficiencies in internal control that are significant within the context of the audit objective and based upon the audit wok performed are stated in the Detailed Audit Findings section of this report.

For further information regarding internal control components and the related principles of internal control, please see Appendix A

Background

The City's efforts to improve IT security and cybersecurity began after the treasury theft in 2011. [redacted] Cyber and other security intrusions are the biggest challenge facing Information Technology department functions, as attacks have become more sophisticated through the years and institutions have suffered major losses and reputational risks as a result of intrusions. The risk of intrusion cannot be eliminated, instead, mitigation remains the priority. [redacted]

The City's first step was to hire a consultant in 2012 to identify deficiencies in the existing technology infrastructure. A security assessment requires sophisticated tools for scanning to determine vulnerabilities and network penetration skills and tools. Clifton Larson Allen (CLA) was engaged in 2012. A timeline for the CLA assessments and key findings is shown below.

[redacted]

[redacted]

The IT department retained the services of Coalfire to remedy issues identified by CLA in 2015. The assignment lasted approximately four years, ending in the summer of 2019. Details of the assignment, costs, and vendor productivity are discussed in the audit findings section.

[redacted]

Audit Results

Coalfire's Impact on the City's Cybersecurity Program

Coalfire, a national Information Technology consulting firm with branches throughout the United States, was retained to assist in cyber and other IT security efforts by the prior Chief Information Officer (CIO). Their consulting efforts spanned several years, beginning in 2015 and ending in October 2019. Funding was requested through the budgetary process and approved by the City Council. The vendor was selected through the Texas Cooperative purchasing program. The table below shows an itemization of Coalfire costs, by purchase order.

PO Number	Date	Purpose	Total Invoices	Total Cost
134144	4/6/2015	Security Program Support	7	$94,905
137759	10/7/2015	Strategic Information Security	17	$243,816
146535	7/6/2016	Cybersecurity Advisory Svc	3	$37,776
148478	9/5/2016	Cybersecurity Advisory Svc	2	$51,085
168998	7/3/2018	APD mobile Security Assessment	2	$10,800
168525	6/7/2018	Information Security Services	4	$57,362
152260	3/2/2016	Information Security Services Bid 17-0082 MO 02282017	13	$335,411
176236	12/21/2018	Cybersecurity Advisory Bid 18-0092 MO 06102918-2	11	$147,707
179780	3/7/2019	IT Project Security Risk Assessment	2	$4,371
		Total		**$983,233**

When Coalfire began their cybersecurity efforts, the City's IT department did not have a designated security team. The 2013 State of the Security assessment by CLA cited many deficiencies in the City's network and cybersecurity. The primary objective for Coalfire was to remedy deficiencies identified by CLA and to serve as security staff for the IT department. The Coalfire efforts were overseen by the prior Chief Information Officer (CIO).

Internal Audit's review of Coalfire activity included the following:

- Review contracts for project scope and deliverables
- Tabulate costs
- Assess contract compliance and status of deliverables
- Assess how Coalfire efforts benefited the current state of the City's Information Security
- Conclude on cost vs. benefits gained from the vendor engagement

Since the Coalfire engagement ended in the summer of 2019, documents and pertinent records were provided by IT staff. Current IT management, the former CIO and Deputy City Manager were interviewed to obtain feedback related to vendor involved projects and deliverables. In addition to the

engagements listed earlier, Coalfire was also contracted to perform a security assessment of specific software used by the Arlington Police Department. This was not included in the current audit scope.

A total of four contracts with Coalfire, spanning from 2015 to 2018, were provided by the IT Department. The contracts typically identified scope of planned services listed as "our understanding" or "scope of work" and deliverables for the project (i.e. individually itemized documents). It is important to note that some of the contracts simply included a scope of work without listing specific deliverables/documents to be provided. However, it appears that a deliverable, or evidence of work completed, was expected based on the verbiage.

The following are examples of *defined scope of work* from Coalfire contracts that are related to IT security and cybersecurity.

The following are *deliverables* included in contract language that are related to IT security and cybersecurity, which were the focus of the current audit.

Professional Standards

There are many established professional standards for IT security and cybersecurity that entities follow when performing duties in these areas. Information Security Audit and Control Association (ISACA) and National Institute of Standards and Technology (NIST) are two such organizations widely accepted by professionals. These standards complement each other and are similar in nature. A combination of frameworks may also be used. For example, ISACA's Control Objectives for Information and Related Technology (COBIT) is used in conjunction with the NIST cybersecurity framework to formulate policy and procedures for individual organizations. The basic cybersecurity framework per NIST standards, which is based on five basic principles, is explained below. It is

intended for use by any entity that wishes to prevent, detect and respond to cyber-attacks. The framework serves as an acceptable IT security methodology to protect a network from intrusion from outsiders.

Identify - Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. Security aspects, such as asset management, governance, risk assessment and management fall under this category.

Protect - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. Security aspects, such as access control, training, data security, data protection processes and maintenance of network equipment fall under this category.

Detect - Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. Security events, such as continuous monitoring and detection processes, such as scanning for timely detection falls under this category.

Respond - Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. Security events, such as response planning, communication, analysis of response methods, mitigation of the event, and future improvements are included in this category.

Recover - Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. Security activity such as recovery planning, improvements based on lessons learned, and communications with stakeholders to restore services are included in this area.

Additionally, there are standards that detail security activity under each section above. These sub level standards dictate security plans customized to individual organizations, based on unique data, equipment, staffing, customer needs, location, risks and financial resources. For example, ISACA standards for an incident response plan (IR), which would fall under the respond section above. IR plans are part of a broader disaster recovery plan and are discussed here for illustrative purposes. An IR plan is a set of tools and procedures that your security team can use to identify, eliminate, and recover from cybersecurity threats. It is designed to help your team respond quickly and uniformly against any type of external threat.

The following is a sample of elements necessary for a successful IR plan:

- Definition of operational, reputational, compliance and financial risks unique to an organization and possible incidents for each type of risk
- Executive Management endorsement
- IR team comprised of members from varying areas of expertise and clear roles and responsibilities for each team member
- A defined communication plan
- Alignment of IR plan to the overall organization disaster recovery plan
- A unique defined response plan for incidents identified

- Regular testing of the IR plan
- An operation plan that defines how incidents are declared and initial steps for information gathering
- A post incident process for lessons learned and process improvement

Audit Assessment

As part of assessing the Coalfire assignment and quality of the work performed, Audit provided the IT department with a list of deliverables and intended scope from the vendor contracts and requested IT provide the respective reports or documents for Audit review. Documents authored by Coalfire included process maps, narratives, and system generated reports. The review of documents was coordinated with additional one on one interviews with IT Management and staff. Audit analysis is discussed below.

- Internal Audit found that many of the Coalfire documents, produced under the deliverable clauses of the contracts, were not ready to be implemented. Most were in draft form, lacking step by step procedures or detailed information applicable to the City of Arlington, which would be necessary for implementation. They primarily consisted of theoretical information, standards published by NIST or ISACA, or simply listed needed elements for a particular program, such as an incident response plan. The documents had not been reviewed or approved by executive management, Human Resources, or the City Attorney's Office. These documents can be regarded as first steps in a workable policy and related procedures.

  Examples are listed below.

  - Access control process flow
  - COA data migration standard
  - COA incident response high level flow
  - Asset classification process flow
  - Security program monitoring and compliance process flow
  - Personnel security process
  - IT service continuity and disaster recovery process flow
  - Data migration plan
  - Vulnerability management process flow
    IT governance model – proposed

- The documents listed below prepared by Coalfire are, conversely, progressive compared to the deliverables mentioned above. These include information useful in policy formulation and implementation. It appears they could be implemented currently, with additional COA specific steps and senior management approval.

  - Account and access management policy
  - Vendor and third-party management policy

- Internal Audit also reviewed two sets of presentations that appear to be proposed training for IT staff or City employees. They are rudimentary in nature. One is a proposal to management regarding what a training program should consist of, and the other presentation, titled "User Security Playbook," is targeted to employees. It includes information pertaining to basic threats and scenarios of incidents, such as a hacking attack and phishing attacks. Audit did not identify evidence of training provided to City staff as a result of the Coalfire efforts.

- During the review of invoices, we were unable to reconcile invoice detail to specific contract clauses or work performed. The descriptions in invoices show general verbiage such as "cyber risk CISO services," "internal audit readiness," "security program operationalization," "identity management," "scheduled billing," and "strategic security management." Explicit evidence of the verification of contract clauses and service delivery prior to paying the vendor was not identified.

- Coalfire staff provided several presentations, related to the state of security at the City, to the City Manager's Office. The presentations listed various threats facing the City and remediation strategies. However, the content of contracts, signed in years prior to the presentations, listed the very same risks as needing mitigation. The contracts listed the remedial activity as part of scope and deliverables. It is important to note the deliverables listed in contracts signed previously would have remedied the vulnerability discussed in the presentations.

- The final CLA risk assessment in February 2015, conducted before the Coalfire engagement, included a detailed remedial action plan for vulnerabilities identified by CLA. The assessment included a cost to cure, based on going rates, to remedy the deficiencies. The cost estimate was shown to be between $219,000 and $367,500. These cost estimates are much less than the amount paid to Coalfire for the above-mentioned contracts.

- IT staff and management attested to attending weekly meetings conducted by Coalfire, to define governance, policy, process and documentation standards. The intention was to establish the incident response process flow and change management. The meetings were less frequent as time progressed (2017 to 2018 timeframe). Staff members interviewed during the audit were unable to provide material evidence of an outcome resulting from these meetings.

Conclusion

As mentioned earlier, Coalfire activity was terminated in October 2019 to pursue another avenue in IT security for the City. Establishment of a more effective, integrated support model is the primary objective for the new direction. [redacted] These individuals were hired through a temporary agency. The cost is expected to be less than that paid to Coalfire. They have been provided with the security findings from CLA and the suggested remedial action plan. The new contract staff members report to the IT Infrastructure Manager and are currently performing the tasks listed below.

[redacted]

The use of outside security contractor assistance in the future is expected to be limited to unique security threats or other security needs with a limited, defined scope and cost limitations. There are no specific audit recommendations associated with the Coalfire engagement, considering the engagement has ended. The current Chief Technology Officer has stated he is committed to better contract management, to include validation and verification of vendor performance and contract compliance. We noted new directives have been issued to IT staff going forward to address the deficiencies.

Current State of Security and Cybersecurity

[redacted]

[redacted]

It is necessary for the IT department to be on the offensive concerning security and cybersecurity. Some aspects of this approach are already in progress. [redacted]

Some of the City's information assets are public information. However, some of the data sets include personal data and require protection. [redacted] Data breaches usually result in the inability to use data, theft of data, or the inability to conduct transactions. This risk is common to all data, regardless of whether it is public or sensitive in nature.

Detailed Audit Findings

Contractor Use of COA Email and Job Titles

A review of Coalfire staff assignments, as they appear in the City's Remedy work order system, indicates the following:

[redacted]

[redacted]

Contractor Background Checks and CJIS Clearance

Coalfire contract workers performed security and cybersecurity related assignments for the City. They were involved in projects related to public safety and participated in other related IT services as systems administrators. The following was noted as a result of a review of their assignments:

- The project team lead who performed public safety software analysis had not been subjected to a required background check and CJIS clearance before access to sensitive data and public safety projects
- A team member, who was given system administrator privileges that resulted in access to departmental shared drives with sensitive data, also did not have background and CJIS clearance prior to access

City of Arlington employees, such as Information Technology staff who have network administrator level access and access to departmental shared drives with sensitive data, are required to submit to a background check prior to employment. The same requirement applies to outside vendors performing tasks associated with sensitive data. Staff that may encounter Police or Fire department (public safety) data are also required to receive Criminal Justice Information Systems (CJIS) clearance and certification prior to being granted access.

CJIS requirements are based on State of Texas and Federal governmental regulations and are mandatory. Access requirements include participants passing a study guide and an exam administered by the City of Arlington Police department.

Individual departments are tasked with obtaining the necessary clearances for staff members and contractors that may come in contact with sensitive data. In this event, it appears the IT department did not request clearances for all Coalfire staff members with access to sensitive data. Four other Coalfire staff had been subjected to the background and CJIS clearance requirements

State and Federal agencies can revoke City of Arlington's access to sensitive public safety systems and data for violating the compliance requirements. Staff members not trained in custodianship of sensitive law enforcement data could misuse or expose data to others.

Recommendations:

4. ***The City Auditor's Office recommends the Chief Technology Officer require all contractor staff encountering sensitive data be subjected to background reviews and CJIS clearance prior to being granted access to such data.***

5. ***The City Auditor's Office recommends the Chief Technology Officer ensure that the CJIS policy on background clearance requirements for all staff members and contractors having access to sensitive information be communicated to IT managers and include the policy and requirements in departmental training efforts to improve compliance.***

[redacted]

[redacted]

[redacted]

Network perimeter security is mandatory in any systems network and is recommended by all existing security standards, such as NIST or ISO. The standards also require routine monitoring of network perimeter and initiating corrective action for deficiencies identified.

[redacted]

City Data Assets & Data Loss Prevention (DLP)

Audit's review of how City data assets are protected from cyber and other security threats indicated the following existing deficiencies.

[redacted]

[redacted]

Data protection begins with policies that categorize data based on sensitivity, definitions of authorized use, and limitations of usage per various standards such as NIST and data security guidelines by ISACA. The next step is monitoring data movement patterns and data traffic within a network, as well as entering and exiting the network. [redacted].

[redacted]

In some instances, DLP tools issue the first alerts of a potential security breach to IT staff, based on movement of data within, to, and from a network. Most attacks are stealth in nature, with some involving the planting of trojans in a network where breaches occur over an extended period of time. It is important to note that authorized users within the City can also download large volumes of data, out of the norm of daily duties, for personal gain. DLP software can detect this as well. Overall, data classification and a DLP program is a key component of an organization's overall security program. Cyber or other security breaches usually result in loss of data. Loss occurs when hackers download data during the attack, or data is illicitly obtained by internal authorized users. Internal threats generally include disgruntled employees or employees misusing data for personal gain.

[redacted]

AUDIT RECOMMENDATIONS AND MANAGEMENT RESPONSE

RECOMMENDATION	CONCUR/ DO NOT CONCUR	MANAGEMENT RESPONSE	RESPONSIBLE PARTY	DUE DATE
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
4. The City Auditor's Office recommends the Chief Technology Officer require all contractor staff encountering sensitive data be subjected to background reviews and CJIS clearance prior to being granted access to such data.	CONCUR	The IT Department will adhere to CJIS requirements for employees and contractors.	Information Technology	09/02/2021

5. The City Auditor's Office recommends the Chief Technology Officer ensure that the CJIS policy on background clearance requirements for all staff members and contractors having access to sensitive information be communicated to IT managers and include the policy and requirements in departmental training efforts to improve compliance.	CONCUR	The IT Department will adhere to CJIS requirements for employees and contractors. The CJIS process includes a bi-annual training that must be completed by contractors and employees.	Information Technology	06/01/2021
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Appendix A
The Five Components and 17 Principles of Internal Control

Control Environment

1. **The oversight body and management should demonstrate a commitment to integrity and ethical values.**
2. **The oversight body should oversee the entity's internal control system.**
3. **Management should establish an organizational structure, assign responsibility and delegate authority to achieve the entity's objectives.**
4. **Management should demonstrate a commitment to recruit, develop and retain competent individuals.**
5. **Management should evaluate performance and hold individuals accountable for their internal control responsibilities.**

Risk Assessment

6. **Management should define objectives clearly to enable the identification of risks and define risk tolerances.**
7. **Management should identify, analyze, and respond to risks related to achieving the defined objectives.**
8. **Management should consider the potential for fraud when identifying, analyzing and responding to risks.**
9. **Management should identify, analyze and respond to significant changes that could impact the internal control system.**

Control Activities

10. **Management should design control activities to achieve objectives and respond to risks.**
11. **Management should design the entity's information system and related control activities to achieve objectives and respond to risks.**
12. **Management should implement control activities through policies.**

Information & Communication

13. **Management should use quality information to achieve the entity's objectives.**
14. **Management should internally communicate the necessary quality information to achieve the entity's objectives.**
15. **Management should externally communicate the necessary quality information to achieve the entity's objectives.**

Monitoring

16. **Management should establish and operate a monitoring mechanism that monitors both internal and external activities that impact the control system and evaluate the results.**
17. **Management should remediate identified internal control deficiencies on a timely basis.**