CITY AUDITOR REPORT

CYBERSECURITY DETECTION AND RESPONSE CAPABILITIES

AUGUST 19, 2021

THIS AUDIT PROJECT WAS CONDUCTED ON SECURITY-SENSITIVE AREAS FOR WHICH KANSAS OPEN RECORDS ACT DISCLOSURE EXCEPTIONS PROVIDED BY K.S.A. 45-221 (a) (12) APPLY. *ACCORDINGLY, DETAILS AND RESULTS IN THESE SENSITIVE AREAS WERE SHARED ONLY WITH CITY MANAGEMENT AND CITY COUNCIL MEMBERS*. FOLLOWING IS A GENERAL OVERVIEW OF THE NATURE, SCOPE AND OBJECTIVES OF THE AUDIT.

BACKGROUND/INTRODUCTION

This cybersecurity project was prioritized by the City Council in the 2021 Audit Calendar, with the goal of assessing the City's capability to detect and respond to potential cyberattacks. Several factors are relevant to keep in mind when considering infrastructure cybersecurity:

Cybersecurity needs and tools are constantly shifting.

Attack methods and actors continually devise new targets and attacks. In response, cybersecurity needs and related tools/techniques change frequently.

The risk of cyberattack is growing rapidly for organizations of all types.

Attacks can come **from a variety of actors and actions,** ranging from foreign governments and international cybercriminals to accidental system malware infection via employee errors. Several **different types** of attack may also occur. According to Cisco, an international technology conglomerate, common types of cyberattacks include: malware/ransomware, phishing, 'man in the middle', denial of service (DOS), Structured Query Language (SQL) injection, Zero-day exploits, and Domain Network System (DNS) tunneling. **For further detail of these cyberattack methods, see the Appendix 1 at page 3.**

Cyberattacks can have multiple costs – financial loss, operating disruption and reputational damage may all be high.

Examples include:

- The March 2018 ransomware hack of the **City of Atlanta**: The City estimated a cost of **$2.7 million in emergency contracts alone**. **Watershed and Municipal Court** departments were the most severely affected; many employees **could not access their computers for 5 days.**[1]
- Solar Winds: In December 2020, Russia is believed to have hacked the systems of the technology company Solar Winds and entered approximately 18,000 customers'[2] systems through code in software patches provided by them. US government entities infiltrated are believed to include the **Department of Homeland Security, the Pentagon, the Department of Energy and US Treasury Department**.[3]

Attackers are present in victim organizations' systems for lengthy periods of time before detection.

In 2020, IBM estimated the average time to identify and contain a breach was 237 days.[4]

Due to these factors, the City of Olathe needs cyberthreat controls and protocols **which achieve maximum protection within its financial and human resource constraints.**

[1] *'Cost of City of Atlanta's cyberattack: $2.7 million – and rising',* Atlanta Journal-Constitution, October 1, 2019, https://www.ajc.com/news/cost-city-atlanta-cyber-attack-million-and-rising/nABZ3K1AXQYvY0vxqfO1FI/

[2] *'Solar Winds: How Russian Spies Hacked the Justice, State, Treasury, Energy, and Commerce Departments'*, CBS News, 60 Minutes; February 14, 2021 https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/

[3] *'What is the Solar Winds Hack and Why Is It a Big Deal?',* Business Insider; December 2020 *https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12*

[4] *'Cost of a Data Breach Report 2020',* IBM Security; https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

AUDIT SCOPE

The scope of this project focused on cyberthreat detection and response protocols/controls established in City systems, as well as management's assessment of the effectiveness of these protocols/controls. Management interviews were used to gather protocol status information. To assess a control or method used in these areas, the following gauges were used:

- sound/common internal control principles
- applicable 'Detect' and 'Respond' functions in the National Institute of Standards and Technology (NIST) *'Framework for Improving Critical Infrastructure Cybersecurity', and*
- to supplement interpretation of the above Framework as needed, applicable sections of NIST Special Publication 800-53 *'Security and Privacy Controls for Federal Information Systems and Organizations'* were consulted

The **NIST Cybersecurity Framework functions/categories in the scope of this review are shown below.**

NIST FRAMEWORK FOR IMPROVING CRITICIAL INFRASTRUCTURE CYBERSECURITY	
Function	**Category**
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

AUDIT OBJECTIVES

The objectives of this audit project were to determine whether City detection and response protocols are established and are assessed by management as having the capability to:

- Detect anomalies/anomalous activity, and have the capacity to understand its potential impact
- Monitor the information system/assets to identify cybersecurity events, and that such monitoring can verify the effectiveness of protective measures
- Ensure awareness of anomalous events through the establishment, maintenance and testing of detection processes and procedures
- Execute and maintain response processes/procedures to ensure response to cybersecurity incidents
- Coordinate response activities with internal and external stakeholders (such as external law enforcement agencies)
- Conduct analysis to ensure that response and support recovery activities are effective
- Perform activities to prevent expansion of an event, mitigate its effects, and resolve the incident
- Incorporate 'lessons learned' from current and previous detection/response activities to improve current organizational response

APPENDIX 1

COMMON TYPES OF CYBERATTACK

For management and the Governing Body's reference and information, below are brief descriptions of the most common types of cybersecurity attacks. [1]

- **Malware** – which breaches a network through a vulnerability, typically hyperlinks or attachments emailed to users, and **includes spyware, ransomware, viruses and so-called 'worms'**. Such an attack can block access to key network components, install malware/harmful software, covertly obtain hard drive information, or disrupt system operation
- **Phishing** – the practice of sending fraudulent communications which appear legitimate to steal sensitive data, such as credit card or login information, *or* to install malware. This threat is increasingly common.
- **Man-in-the-middle attack** – which allows attackers to insert themselves into a 2 party transaction to filter or steal data. Two common points of entry for this attack are unsecure public WiFi, and occurrence as a result of an initial malware attack.
- **Denial of service** – this attack floods systems/servers/or networks with high traffic volume to exhaust bandwidth; legitimate uses and requests cannot be fulfilled. One subcategory of this attack type is a 'distributed' denial of service attack (DDOS), which uses multiple compromised devices.
- **SQL injection** - A 'Structured Query Language' (SQL) attack occurs when malicious code is inserted into a server using SQL and forces the server to reveal secure/confidential information.
- **Zero-day exploit** – A zero day exploit is launched using a specific time window *after* a network vulnerability is announced by network services/providers, but *before* a patch is issued/implemented.
- **DNS Tunneling** – This attack utilizes the domain name system (DNS) protocol, which normally helps users and network devices discover websites using 'readable' hostnames instead of numeric IP addresses. This type of attack can use DNS system ports for malicious purposes, such as disguising outbound traffic to export/exfiltrate data from a compromised system to the attacker's infrastructure. It can also be used by an attacker to command and control of a compromised system.

[1] '*The Most Common Security Cyberattacks',*
https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html