Cybersecurity

Department of Innovation and Technology

OBJECTIVES

This audit was conducted to determine whether effective controls are in place that would help prevent, deter, and/or respond to cyberattacks.

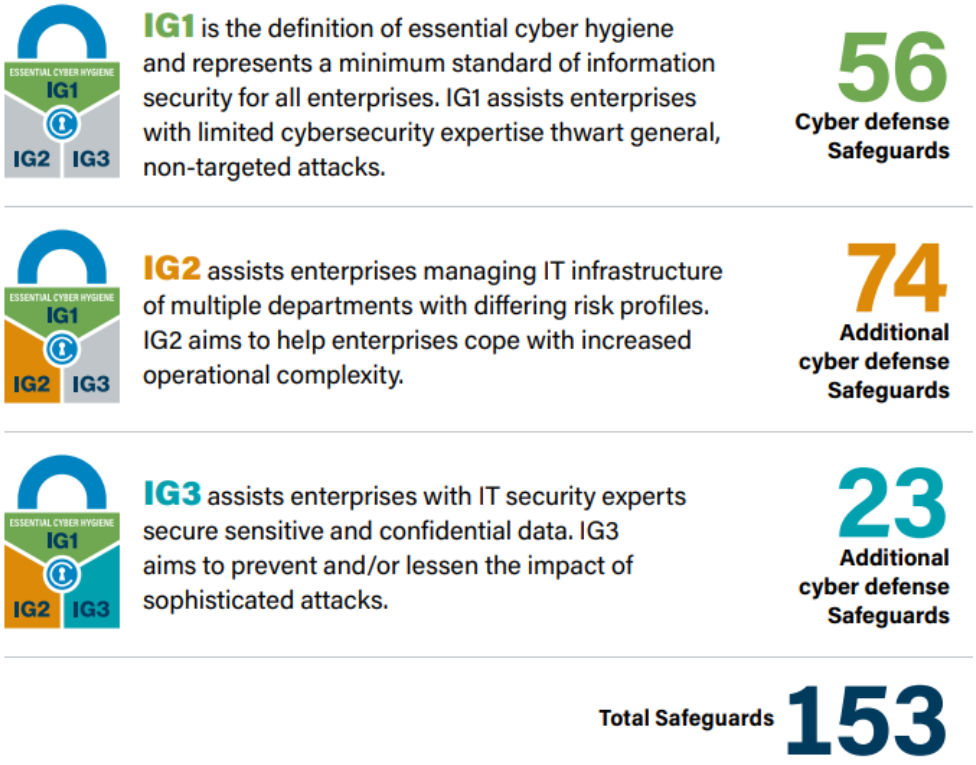
BACKGROUND

According to a StateScoop article, *Cyberattacks on State and Local Governments Rose in 2023*, the Center for Internet Security found that cyberattacks on state and local governments increased from 2022 to 2023. This finding stems from the results of its *2022 Nationwide Cybersecurity Review*, which surveyed more than 3,600 state, local, tribal, and territorial government organizations on cybersecurity preparedness. The report focused on the first eight months of 2022 and 2023 and found that malware attacks increased by 148%, while non-malware cyberattacks increased by 37%. The report also found a 313% increase in endpoint security services incidents, such as data breaches, unauthorized access and insider threats.

As the threat of cyberattacks continue to rise and evolve, organizations are taking steps to address these challenges and further improve their cybersecurity practices. For example, there are several IT frameworks that provide guidelines, best practices, and controls to help organizations manage and reduce their cybersecurity risk. For example, the National Institute of Standards and Technology (NIST) has developed frameworks, such as the NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, and the NIST Cybersecurity Framework 2.0. The Center for Internet Security has developed the CIS Critical Security Controls (CIS Controls), which is the framework that the Department of Innovation and Technology (DoIT) had chosen to align its practices with.

The CIS Controls are a recommended set of actions and best practices to improve cybersecurity, which consists of 18 controls and 153 safeguards. Each CIS Control consists of several safeguards or specific actions that an organization should take in order to implement the control. Implementation Groups (IGs) were developed to prioritize implementation of the safeguards for each CIS Control. IGs are based on an organization's risk profile and available resources. They are self-assessed categories that are divided into three groups: Implementation Group 1 (IG1), Implementation Group 2 (IG2), and Implementation Group 3 (IG3). IG1 is defined as "essential cyber hygiene" and includes those safeguards that organizations should implement in order to defend against the most common cyberattacks. Each IG builds upon the previous one. For example, IG2 includes all safeguards in IG1 and IG3 includes all safeguards in IG1 and IG2.

The figure below illustrates the different implementation groups and how many safeguards are included in each group:



For purposes of this audit, DoIT was evaluated against the safeguards described in IG2. See the Appendix for a description of the 18 CIS Controls.

SUMMARY OF OBSERVATIONS

1. DoIT does not have adequate controls in place to ensure its enterprise asset inventory is accurate and up to date.

2. DoIT does not have adequate controls in place to ensure its software inventory is accurate and complete.

3. DoIT has not fully implemented all the safeguards to ensure data is protected and managed appropriately.

4. DoIT has not fully implemented all the safeguards to ensure enterprise and software assets are securely configured.

5. DoIT has not fully implemented all the safeguards to ensure that credentials for user accounts are appropriately assigned and managed.

6. DoIT did not always retain documentation authorizing the creation of administrator and service accounts.

7. DoIT does not have written policies and procedures for its audit log management process.

8. DoIT does not restrict the use of email client plugins.

9. DoIT's data backup and recovery procedures are not reviewed and updated on an annual basis.

10. DoIT does not implement an internal firewall between all servers and end-user devices that are connecting to the City's network.

11. DoIT has not fully implemented all the safeguards to ensure third-party service providers are appropriately evaluated.

CONCLUSION

In our opinion, DoIT has implemented some effective cybersecurity measures that would help prevent, deter, and/or respond to cyberattacks. However, there are several safeguards described in the CIS Controls that DoIT has not yet developed and implemented or could be further improved.

Due to the sensitive nature of the findings contained in the audit report, detailed information has been limited to city and department management as well as the Audit, Finance, and Enterprise Committee.

SCOPE

The scope of the audit was the period between January 1, 2023 through December 31, 2024.

METHODOLOGY

To accomplish our objective, we performed the following:

- Interviewed department personnel to gain an understanding of the internal controls in place to ensure compliance with the safeguards described in the CIS Controls.
- Performed a walk-through of the department's asset management system to gain an understanding of how enterprise and software assets are tracked, inventoried, and maintained.
- Reviewed city and departmental policies and procedures, such as the following:
    - Data privacy and data governance.
    - Virtual private network (VPN) and remote work.
    - Granting and revoking user access.
    - Application development, including the procedures for testing, reviewing, and retiring applications.
    - Vulnerability management, including roles and responsibilities and vulnerability identification and remediation.
- Reviewed department standards for secure configuration, vulnerability management, and digital kiosk devices.
- Reviewed the department's Cyber-Incident Response Plan and Disaster Recovery and Business Continuity Plan, including backup and restoration procedures.
- Reviewed tools that are utilized to identify and monitor assets, including installed software, that connect to the City's network.
- Verified firewalls were implemented to help filter traffic between some network segments and end-user devices connecting through a VPN solution.
- Reviewed inventory listings of enterprise assets, including software applications, user accounts, and service providers, including third-party software components.
- Selected a sample of employee user accounts, including administrative and service accounts, to determine whether access was properly authorized.
- Selected a sample of terminated employees to determine whether their access was revoked in a timely manner.
- Verified enforcement of a VPN and multi-factor authentication (MFA) for administrative and remote access, including when accessing City resources on end-user devices.
- Assessed the frequency of vulnerability scans and reviewed vulnerability scan results.
- Reviewed tools used to ensure automated patch updates are being performed on applications and operations systems.
- Reviewed examples of audit logs that are collected, reviewed, and retained.

- Reviewed tools used to aggregate threat intelligence and block access to malicious domains and unnecessary file types.
- Verified the deployment of anti-malware software, including the use of behavior-based detection tools.
- Reviewed documentation of automated data backups and recovery tests.
- Reviewed network infrastructure diagrams and baseline configuration templates.
- Verified the deployment of network monitoring tools, such as a host-based intrusion detection system and a network intrusion detection system.
- Reviewed network traffic flow logs to ensure logging and monitoring were in place and used for threat detection.
- Reviewed security awareness training materials to verify that a formal training program was in place, including real-time status reports of employees that do not complete the annual training.
- Examined service provider contracts to determine whether they included security requirements.
- Reviewed training certificates of application development personnel.
- Reviewed tools used to manage and prioritize software vulnerabilities, including those identified on applications developed in-house.
- Examined documentation of the department's annual incident response exercise that is designed to evaluate the City's preparedness during an actual event.
- Reviewed documentation of penetration tests, including the final reports detailing the vulnerabilities identified and the remediation steps recommended.

AUDIT 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.

Appendix

The CIS Critical Security Controls consist of 18 Controls. The following is a description of the recommended set of actions for each of the Controls:

Control 01 — Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.

Control 02 — Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Control 03 — Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Control 04 — Secure Configuration of Enterprise Assets and Software

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Control 05 — Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Control 06 — Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Control 07 — Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Control 08 — Audit Log Management

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Control 09 — Email and Web Browser Protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Control 10 — Malware Defenses

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Control 11 — Data Recovery

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Control 12 — Network Infrastructure Management

Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.

Control 13 — Network Monitoring and Defense

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Control 14 — Security Awareness and Skills Training

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Control 15 — Service Provider Management

Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Control 16 — Application Software Security

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Control 17 — Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Control 18 — Penetration Testing

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.

The full version of the CIS Critical Security Controls can be found at CIS Critical Security Controls (cisecurity.org).

The City Auditor's office provides audit, consulting, and investigative services to identify and minimize risk, maximize efficiencies, improve internal controls, and strengthen accountability to Mesa's citizens. We serve as an independent resource to City Management and the City Council, to provide them with timely, accurate, and objective information, assurances, and recommendations pertaining to City of Mesa programs and activities.

Audit Team

Michelle Hute, Senior Internal Auditor

City Auditor

Joseph Lisitano, CPA, CIA

Mesa City Auditor's Office

Phone: 480-644-5059

Email: auditor.info@mesaaz.gov

Website: https://www.mesaaz.gov/government/city-auditor

Copies of our audit reports are available at:

https://www.mesaaz.gov/government/city-auditor/audits