Review of Select Cybersecurity Processes
Phase II: Malware (Ransomware)

Project #2022.07
June 2024

Executive Summary

The objective of the audit was to determine whether existing processes and controls were sufficient to safeguard the agency from malware. The review focused primarily on ransomware and addressed state and federal information security standards and guidance, internal policies and procedures, as well as other relevant laws, rules, and regulations. The scope of the audit covered fiscal year 2023 (September 1, 2022, to August 31, 2023), as well as any other related time periods.

Overall, our review found that processes and controls have been established to provide assurance that the agency's information resources are safeguarded in accordance with state and federal information security standards and guidance. However, certain processes and controls should be strengthened to further ensure the agency is protected from malware.

To minimize security risks, auditors communicated details about the audit separately to the Board, Executive Administration, and management in a confidential report. Auditors provided recommendations to address the issues identified during this audit. Management agreed, and provided their responses and the estimated implementation dates for each of the recommendations.

Pursuant to Standard 9.61 of the U.S. Government Accountability Office's Government Auditing Standards, certain information was omitted from this document because that information was deemed to present potential risks related to public safety, security, or the disclosure of private or confidential data. Under the provisions of Texas Government Code, Section 552.139, the omitted information is also exempt from the requirements of the Texas Public Information Act.

Objectives, Scope, and Methodology

Objective

The objective of the audit was to determine whether existing processes and controls were sufficient to safeguard the agency from malware. The review focused primarily on ransomware and addressed state and federal information security standards and guidance, internal policies and procedures, as well as relevant laws, rules, and regulations.

Scope and Methodology

The scope of the audit covered fiscal year 2023 (September 1, 2022, to August 31, 2023), as well as any other related time periods.

The methodology for the audit consisted of a review of the following information:

- Texas Government Code, Chapter 552.
- Texas Government Code, Chapter 2054.
- Title 1, Texas Administrative Code, Chapter 202.
- DIR's Data Classification Guide.
- DIR's Security Control Standards Catalog.
- DIR's Cybersecurity Framework Control Objectives and Definitions.
- Agency Information Technology Policies and Procedures.
- Disaster Recovery and Incident Response Plans.
- Application data maintained in the systems.

Tests and procedures included the following:

- Interviewed management and staff.
- Reviewed applicable statutes, rules, laws, and requirements.
- Reviewed agency policies and procedures.
- Examined documentation pertaining to change management, patch management, software configuration, vulnerability assessment, vulnerability management, security incident reporting, and security incident response processes.
- Tested a sample of change tickets for security application changes to determine whether they were approved in accordance with policy.
- Reviewed annual disaster recovery tabletop exercise.
- Reviewed third-party (external consultant) annual controlled penetration test and assessment results.
- Evaluated security incident monthly reports to DIR.

This engagement was conducted in accordance with *Generally Accepted Government Auditing Standards* and the *International Standards for the Professional Practice of Internal Auditing*. These 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 observations and conclusions based on our audit objectives.

The audit team consisted of:

David Ramos
Nicky Carter, CICA
Michelle Cooper, CGAP, CFE, CICA
Nicole Campbell, CIA, CISA

Closing

We would like to express our appreciation to management and personnel for their cooperation and assistance provided to the internal audit staff during this review. For questions or additional information concerning this report, please contact Nicole Campbell at (512) 463-7978.

Report Distribution

Internal Distribution

Board's Office
Brooke T. Paup, Chairwoman
Patrick Lopez, Chief of Staff to Chairwoman Paup
George B. Peyton V, Board Member
Adrianne Evans, Chief of Staff to Board Member Peyton
L'Oreal Stepney, P.E., Board Member
Kerry Niemann, Chief of Staff to Board Member Stepney

Executive Administrator's Office
Bryan McMath, Interim Executive Administrator
Kathleen Ligon, Interim Assistant Executive Administrator

Program Area
Edna Jackson, Deputy Executive Administrator, Operations and Administration
Darrell Tompkins, Chief Information Officer, Director of Information Technology
Angela Gower, Information Security Officer

External Distribution

Legislative Budget Board
audit@lbb.texas.gov

Governor's Office of Budget, Planning, and Policy
budgetandpolicyreports@gov.texas.gov

State Auditor's Office
iacoordinator@sao.texas.gov