Office of the Internal Auditor

AUDIT REPORT

October 2022

Vulnerability and Patch Management Audit

CITIZENS
PROPERTY INSURANCE CORPORATION

Table of Contents: Page

Executive Summary

Appendix

Executive Summary

Background

As cyber threats continue to grow in sophistication, organizations face a persistent challenge in protecting their systems against the threat of malicious actors. The average cost of a data breach rose to $4.24 million in 2021, according to a sample of 537 victims of data breaches (Ponemon Institute), while 45% of US companies suffered a data breach in 2021 (Thales Data Report). Cyber threats ranked first among a global survey of 7,400 IT audit leaders in 2021 (Protiviti).

Vulnerability monitoring has been identified as an essential process for guarding against cyber threats. It ranks 7th in the CIS Critical Security Controls (CIS Controls), a prioritized list of specific and actionable ways to prevent and detect cybersecurity attacks. The National Institute of Standards and Technology (NIST) recognized the CIS Controls as a method for implementing its standards.

Vulnerability management includes two areas of primary focus: vulnerability monitoring/remediation and patching. Vulnerability monitoring consists of scans of the network administered by Security, review of other sources, and subsequent coordination with teams throughout IT to remediate issues identified. Patching implements vendor-recommended remediations of published vulnerabilities specific to their technologies.

Objectives and Scope

The objective of the audit was to review vulnerability and patch management policies, procedures, and practices to ensure that the processes are working as intended to timely close security gaps which could potentially be exploited and reduce the risk level to an acceptable level.

The scope of the audit included:

Vulnerability Scanning and Remediation

- Compare the design and implementation of the vulnerability monitoring program to best practices
- Test the coverage of the Citizens' environment, including the IP ranges scanned, as well as the completeness of agents deployed
- Assess the prioritization of vulnerabilities and response to critical, emerging risks
- Test the timeliness and tracking of vulnerability remediations
- Evaluate the process for mitigating vulnerabilities that cannot be remediated
- Appraise the risk acceptance process, including continuous monitoring and reporting
- Determine the effectiveness of reporting to leadership
- Limited assessment of the use of penetration testing

Patching

- Technologies reviewed include servers, clients, network devices, hypervisors, and databases
- Compare the design of each team's patching processes
- Inspect the status of patches for each technology
- Evaluate the process for prioritization of patches and risk assessment

Executive Summary

- Assess reporting, including areas covered and distribution
- Evaluate the consideration of the impact on business processes in determining when to patch
- Compare the process for testing patches to best practices.

Results

Internal audit completed the assessment of vulnerability and patch management and noted the following positive practices:

- IT regularly performs vulnerability scanning utilizing best-in-class external software solutions.
- IT teams attend weekly meetings to review high-priority vulnerabilities, and immediate remediation starts.
- End-of-life asset classes are acknowledged as such by IT and reviewed for expedited retirement where possible and risk mitigation when retirement is not yet possible.
- Separate external organizations performed the most recent biennial penetration tests. Critical vulnerabilities noted in penetration testing reports are addressed without delay.

Results of our assessment of the vulnerability and patch management indicated that there is a need to:

- Formally develop reporting of tracking and metrics around vulnerability and patch management
- Reassess penetration testing frequency based on risk assessment of the asset class

In addition, some improvement opportunities to increase the efficiency and effectiveness of the vulnerability and patch management were considered and discussed with Management.

We want to thank Management and staff for their cooperation and professional courtesy throughout this audit.

Distribution

Addressee(s) Thomas Dubocq, Director – IT Infrastructure
Wendy Emanuelson, Director – IT Security & Risk

Business Leaders:
Barry Gilway, President/CEO/Executive Director
Kelly Booten, Chief Operating Officer
Aditya Gavvala, VP – IT Services and Delivery
Robert Sellers, VP – Chief Technology Officer

Audit Committee:
JoAnn Leznoff, Citizens Audit Committee Chair
Carlos Beruff, Citizens Audit Committee Member and Chairman of the Board
Scott Thomas, Citizens Audit Committee Member

Following Audit Committee Distribution:
The Honorable Ron DeSantis, Governor
The Honorable Jimmy Patronis, Chief Financial Officer
The Honorable Ashley Moody, Attorney General
The Honorable Nikki Fried, Commissioner of Agriculture
The Honorable Wilton Simpson, President of the Senate
The Honorable Chris Sprowls, Speaker of the House of Representatives

The External Auditor

Completed by Protiviti Inc, and Ajay Kumar, Director of Internal Audit
Under the Direction of Joe Martins, Chief of Internal Audit