OFFICE OF THE INTERNAL AUDITOR

CITIZENS PROPERTY INSURANCE CORPORATION

INTERNAL AUDIT

Advisory Memorandum

IT Security and Risk Incident Response Exercise

February 9, 2021

Memorandum Number: 2021-MAS-04 IT Security and Risk Incident Management Exercise Advisory

Advisory Memorandum

Background

An incident response program and plan are components of IT Security which assist IT and business staff in identifying, responding to, and recovering from cybersecurity incidents. The objective of an incident response plan is to rapidly identify potential threat events, have procedures in place to minimize or contain the damage, mitigate the weaknesses that were discovered and return to normal operations. An effective response process can act to significantly reduce the cost and / or reputational damage of an incident.

To strengthen the incident response program, periodic tests or exercises are performed against the established procedures to validate that the response procedures operate as intended. Training is also provided to staff who may be required to execute response-related tasks. To this end, a training session and a discussion-based tabletop exercise were recently facilitated by a third-party vendor so that IT and business staff could validate roles, responsibilities, coordination, assessment, and decision-making in a simulated threat scenario and then assess their actions and results.

The IT Security and Risk department within Enterprise Operations, with collaboration from the Privacy Officer, provides oversight and administration of the incident response program and plan documents. The team schedules periodic exercises with technical and business stakeholders to test the plan and makes suggested improvements to provide reasonable assurance toward plan execution when needed.

Objectives and Scope

Internal Audit was asked to provide advisory services by participating in the incident response exercise, attending the post exercise meeting, and providing feedback to IT regarding:

- Whether the process followed in the exercise met the intent of the Citizens Cybersecurity Incident Response Plan (CSIRP), the Enterprise Data Incident Response Plan (EDIRP) and the CSIRP Checklist
- Strengths and opportunities for improvement noted during the exercise
- Validity of IT observations and recommendations drawn from the exercise
- Completeness of plan documents

Results

Results from our participation in the exercise and post exercise review meeting indicate that the exercise objectives were fully met. We observed the following related to the exercise and plan documents:

Strengths

- The Cybersecurity Incident Response Plan, Enterprise Data Incident Response Plan and CSIRP Checklist were reasonably followed as the tabletop exercise was conducted.
- Formal training provided by the third-party vendor as part of the exercise afforded an overview of incident management to staff who may not have participated in a test event previously.

Advisory Memorandum

- The post exercise team meeting resulted in the identification of some sound areas of improvement and IA agrees with the items noted, specifically providing the team the opportunity to either participate in a functional exercise using a simulated environment or perform steps to validate current logs and backups, communications templates, call tree lists, vendor availability, etc. The exercise could also include cross-over to the Enterprise Data Incident Response Plan for a mock data breach scenario.

Opportunities

- Consider expanding the documentation in the CSIRP and EDIRP plans to include the process steps for recording all facts related to the incident including system events, conversations, individuals added to the team, date and time stamps, communications sent, vendors engaged, and other relevant information that will serve as a log of the event for internal and potential legal purposes. According to NIST, documenting the events can lead to a more efficient, more systematic and less error-prone handling of the problem. Include a documentation retention period for logs and evidence as part of the incident management materials.
- Activating the EDIRP is noted as a potential step in the Containment phase of the CSIRP document, depending upon whether or not a privacy risk exists. Consider adding this same step to the Detection and Analysis phase of the document as well to provide appropriate breach coverage sooner in the response if needed.
- Consider additional training for those individuals who may be requested to fulfill the role of Incident Manager to broaden the number of individuals who can provide this expertise.
- Consider development of an Incident Response Program summary page reflecting overall program status. Summary components may include, but are not limited to: relevant policies, standards and plan documents; tabletop and functional exercises completed and planned; formal training provided and planned; third party vendors contracted to assist with response events; action items in progress; relevant metrics; and current and targeted program maturity levels agreed by IT management.
- Whenever a contact list is created or updated, ensure all plan documents are updated as appropriate or include a reference to the updated list to ensure accuracy and consistency.

We would like to thank management and staff for their cooperation and the opportunity to provide advisory services.

Distribution

Addressee(s) Carlos Rodriguez, Director, IT Security and Risk

Addressee(s) **Business Leaders:**
Barry Gilway, President/CEO/Executive Director
Kelly Booten, Chief Operating Officer
Robert Sellers, V.P., Chief Technology Officer
Christine Turner Ashburn, Chief, Communications, Legislative & External Affairs
Mark Kagy, Acting Inspector General

Audit Committee:
Bette Brown, Citizens Audit Committee Chair
Carlos Beruff, Citizens Audit Committee Member and Chairman of the Board
Marc Dunbar, Citizens Audit Committee Member
Carlos Lopez-Cantera, 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 Karen Wittlinger, Director, Internal Audit, and Gary Sharrock, Internal Audit Manager
Under the Direction of Joe Martins, Chief of Internal Audit