CITIZENS
PROPERTY INSURANCE CORPORATION

Office of the Internal Auditor

Confidentiality
Integrity
Ethics
Objectivity
Competency

AUDIT REPORT

Network Architecture and Design

August 31, 2016

Report Number: 2016-AUD-IT-01 Executive Distribution

Table of Contents: Page

Executive Summary

Appendix

Executive Summary

Background

A network is a group of computers, peripherals, applications, databases, data, voice devices and video devices which are connected by communication mediums. When the devices are in close proximity, such as in a building, the network is referred to as a Local Area Network (LAN). When the devices are in two or more distant locations, the network is referred to as a Wide Area Network (WAN).

But networks bring with them security risks which, if mitigated, allow the benefits of communication to outweigh the risks. For 2016, top security threats for networks include:

- Extortion hacks (ransomware)
- 'Hacktivism' (releasing corporate information to humiliate, shame or bring unwanted attention to an organization)
- Attacks that change or delete corporate data
- Theft of Personally Identifiable Information (PII)
- Denial of Service attacks (DOS) (overloading websites with requests for service, rendering the site unavailable)

Network architecture refers to the layout of the network infrastructure, consisting of the hardware, software, connectivity, communication protocols and mode of transmission, such as wired or wireless. Network design refers to the planning of the implementation of the computer network infrastructure. Typically, network design includes the following:

- Logical map of the network to be designed
- Cabling structure
- Quantity, type and location of network devices (router, switches, servers)
- IP addressing structure
- Network security architecture and network security processes

At Citizens, network architecture and design is the responsibility of the network team. The network team is comprised of a supervisor and four staff, and reports to the Director of IT Infrastructure. In addition to architecture and design, the network team is also responsible for maintaining and monitoring the network infrastructure to ensure that network services are available, provide adequate performance and are secure for all users. The network team also administers network level security such as firewalls, routers and intrusion prevention systems to protect Citizens information systems and users from cybersecurity threats originating from the Internet.

Citizens currently has four office locations and two data centers which have Local Area Networks, interconnected by a Wide Area Network to provide data, voice and video communication between the locations. Citizens is also connected to the Internet to allow independent agents, customers, vendors and employees access to Citizens information systems as they are authorized, public access to the external website, email and other Internet-based activities.

Network technology and components are constantly evolving and improving, and it is important for organizations to keep pace with these changes to ensure ongoing vendor support, improve performance and security, and reduce costs. Examples of these changes implemented by the network team over the past several years include:

- Migrated to MyFloridaNet, enterprise infrastructure based on a Multi-Protocol Label Switching (MPLS) technology providing improved security and robust connectivity resulting in a highly available (HA) and highly reliable (HR) statewide communication network.
- Implemented logical network switches based on fewer physical devices which reduced the total cost of ownership.
- Implemented FCoE (Fiberchannel over Ethernet) which allows enterprise disk storage data to move over Ethernet, resulting in faster speeds and reduced total cost of ownership.
- Implemented an additional layer of security for applications by implementing a web application firewall.
- Relocated network connections and upgraded network devices as part of the relocation of the corporate data center to the CSX co-location facility and the consolidation of the Jacksonville offices.

For 2016 the network team has 12 projects planned including 7 for enhancements, 4 for lifecycle updates to network devices, and 1 to evaluate a new system to improve mobile device security and management.

The network team has a goal of providing 95% or more network uptime (measured by duration of Service Desk tickets for network events divided by the total time in period).

Audit Objective and Scope

The objective of this audit was to assess the network architecture and design from a security perspective and to determine if adequate security mechanisms were in place and operating effectively.

Based on the outcome of procedures performed during the fact finding phase of this audit, OIA selected the following areas for testing during fieldwork:

- Network architecture and design including the use of firewalls to create Demilitarized Zones (DMZ's), segmentation, placement of Intrusion Prevention Systems (IPS), routers and other network devices.
- Configuration (hardening) of network devices and administrative access to network devices
- Remote access to the corporate internal network
- Logging and monitoring of network devices including periodic firewall rule reviews
- Physical access to network cabling and devices at the EverBank Center building
- Capacity planning/management

Special Note: Certain portions of this audit were conducted as attorney-client relationship with Citizens' Privacy Officer. As such, these portions of the audit are confidential under 627.351(6)(x)1.d., Florida Statutes.

Management's Assessment and Reporting on Controls

OIA provided management an opportunity to share known control weaknesses and their plans to remediate them. This process is intended to foster an environment whereby management and staff conduct periodic proactive reviews of controls and are aware of the risks to the business. It also enables OIA to focus its audit efforts on areas where it can add value to the organization.

At the start of the audit, IT Security management shared the following control weaknesses and remediation plans with OIA:

- The 2007 IT Security Policy is considered as the current policy. This policy is known to be outdated, but does include network security policies and standards relevant to the business at that time. An IT Security Strategic Plan was developed in October 2015 which comprises goals and associated initiatives including a goal to “Develop, Approve and Promote an Enhanced Comprehensive IT Security Policy Suite”. A revised policy and approximately 90 associated standards are being developed and are targeted for completion and approval by year-end 2016. Implementation will be expected upon approval with informal gap analyses and implementation responsibilities assumed by IT functional managers.

Audit Opinion

Based upon our audit work, it is OIA’s opinion that the overall effectiveness of the processes and controls evaluated during the audit is rated as **Needs Improvement.**

We found that the network is operating well, serving the needs of the organization and no significant deficiencies in its architecture or design were noted. In particular, there is ample capacity for current needs and peak demands, and there is an on-going effort to improve performance and reduce costs. The network team appears to be well qualified and committed to process improvement.

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. For security reasons, we opted not to fully disclose the details associated with issues related to those controls. Issue owners have provided management action plans and have begun developing corresponding corrective measures.

We would like to thank IT Management and especially the network team for their cooperation and professional courtesy throughout the course of this audit.

Appendix

Definitions

Audit Ratings

Satisfactory

The control environment is considered appropriate and maintaining risks within acceptable parameters. There may be no or very few minor issues, but their number and severity relative to the size and scope of the operation, entity, or process audited indicate minimal concern.

Needs Minor Improvement:

The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate some minor areas of weakness in the control environment that need to be addressed.

Needs Improvement:

The audit raises questions regarding the appropriateness of the control environment and its ability to maintain risks within acceptable parameters. The control environment will require meaningful enhancement before it can be considered as fully effective. The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate some noteworthy areas of weakness.

Unsatisfactory:

The control environment is not considered appropriate, or the management of risks reviewed falls outside acceptable parameters, or both. The number and severity of issues relative to the size and scope of the operation, entity, or process being audited indicate pervasive, systemic, or individually serious weaknesses.

Appendix

Distribution

Addressee Curt Overpeck, Chief Information Officer

Copies **Business Leaders:**

Barry Gilway, President/CEO/Executive Director
Kelly Booten, Chief – Systems and Operations
John Rollins, Chief Risk Officer
Dan Sumner, Chief Legal Officer & General Counsel
Christine Turner Ashburn, VP-Communications, Legislative & External Affairs
Robert Sellers, VP – IT Infrastructure and Operations
Cherri Linn, Director – Facilities Management and Real Estate
Mario Andrade, Director – IT Infrastructure
Mitch Brockbank, Director – IT Security and Risk
Bruce Meeks, Inspector General
Chuck Bowen, Counsel/Privacy Officer

Audit Committee:

Juan Cocuy, Citizens Audit Committee Chairman
Bette Brown, Citizens Audit Committee Member
Jim Henderson, Citizens Audit Committee Member

Following Audit Committee Distribution:

The Honorable Rick Scott, Governor
The Honorable Jeff Atwater, Chief Financial Officer
The Honorable Pam Bondi, Attorney General
The Honorable Adam Putnam, Commissioner of Agriculture
The Honorable Andy Gardiner, President of the Senate
The Honorable Steve Crisafulli, Speaker of the House of Representatives

External Auditors - Dixon Hughes Goodman LLP

Audit Performed By

Auditor in Charge	Gary B. Sharrock, Manager – IT Audit
Audit Director	Karen Wittlinger, Director – IT Audit
Under the Direction of	*Joe Martins* *Chief of Internal Audit*