CENTRAL FLORIDA EXPRESSWAY AUTHORITY

protiviti®
Risk & Business Consulting.
Internal Audit.

Executive Summary of the 2017 Vendor Security Review

Central Florida Expressway Authority

September 2016

protiviti
Risk & Business Consulting.
Internal Audit.

Table of Contents

I. Executive Summary 1

I. Executive Summary

Background

During the period between August 1 to September 2, 2016, Internal Audit ("IA") performed a Vendor Security Review for the Central Florida Expressway Authority ("CFX"). This is the first review of vendor security that IA has conducted at CFX. The review focused on vendor IT connections entering the CFX environment and vendor systems within the CFX environment. CFX vendors play an important role as they perform a variety of critical duties including database management, web development, Intelligent Transportation Systems ("ITS") hardware maintenance, fiber optic network support, engineering, marketing, toll operations and more. The CFX and ITS environments share network equipment that allows communication between the networks, though each is a distinct environment. Though both utilize vendors, the CFX IT environment is larger, making up approximately 90% of the IT systems within CFX. ITS comprises approximately 10% of the IT systems within CFX, and is the area to which vendors connect to maintain systems on the roadways, or systems that support roadway systems.

Scope and Approach

The focus of this review had two (2) primary components. First, IA reviewed vendor IT connections coming into the CFX environment, and second, IA reviewed security configurations of vendor systems within the CFX environment. Specific steps to accomplish these objectives are described here:

- To assess vendor connections into the CFX environment, IA:
  - Established an inventory of vendors with whom CFX exchanges data. In so doing, IA confirmed relevant attributes about each connection, including:
    - The type of connection used (e.g., web URL, Secure File Transfer protocol (SFTP), hosted portal, system-to-system connectivity, etc.)
    - The nature and volume of the data exchanged
  - Identified the appropriate CFX business owner for each connection and discussed the security processes and controls in place to protect data in transit and once it arrived at its destination.
  - Executed specific procedures to test the security controls in place including:
    - Security of the connection
    - Access controls
    - Logging and monitoring

- To assess vendors systems within the CFX environment, IA:
  - Established an inventory of vendors that have placed systems within the CFX environment
  - Identified the appropriate CFX business owner for each vendor system (or group of systems) that exists within the CFX environment and discussed the security processes and controls in place to protect data on those systems.
  - Executed specific procedures to validate the design and operating effectiveness of the security controls in place including
    - System configurations (system hardening, operating system patching, software updates)

  - Access controls
  - Logging and monitoring

In order to accomplish this review, Internal Audit:

- Interviewed key personnel (i.e. CFX Security Manager, ITS Domain Administrator, IT Administrators)
- Performed a Risk Analysis of vendors in the environment to determine which to sample
- Performed a sample-based review of high-risk vendor access
- Reviewed documentation associated with the vendor access request, authorization, and approval process
- Performed walkthroughs of CFX access control systems (i.e. Active Directory, Juniper Radius, and the WatchGuard Firewall)
- Reviewed system configurations for a sample of vendor systems (or systems to which vendors had access)
- Obtained an understanding of how vendor access is provisioned, controlled, and monitored

The vendor systems and connections assessed as part of this review are:

- Transcore – Manages databases and servers in the environment
- Atkins – Manages and maintains systems within the ITS environment
- Kapsch – Manages and maintains systems within the ITS environment
- Evolve – Manages and maintains websites within the CFX environment
- Carousel – Provides support for network infrastructure in the CFX environment
- AEcom – Collects cash tolls for CFX on the roadways

Summary of Findings

As a result of this review, Internal Audit identified six (6) observations specific to the ITS environment that should be addressed in order to strengthen the overall security of vendor IT connections that come into CFX's ITS environment and the security configurations on vendor systems that exist within the CFX ITS environment (no observations were identified within the CFX IT environment). The observations are grouped into the following three (3) high-level topics:

- Vendor Access and Privileges
- Vulnerability Management
- System Configuration Settings

Recommendations

The following high-level recommendations should be considered in order to address the topics above:

- Review Vendor Access and Privileges
- Require Formal Vulnerability Management Processes
- Enhance System Configuration Settings

Status of Completion

As of the time of this report, five of the six observations have been remediated.