# IT Endpoint Management (20-02)

Terry Follmer, VP of Internal Audit

**Distribution List:**
Capital Metro Board of Directors
Randy Clarke, President and CEO
Kerri Butcher, EVP, Chief Counsel & Chief of Staff
Donna Simmons, EVP, Administration & EEO Officer
Reinet Marneweck, EVP, Chief Financial Officer
Dottie Watkins, Chief Customer Officer & COO
David Dech, VP, Rail Operations
Ken Cartwright, VP, Capital Projects
Jane Schroter, VP, Chief Information Officer
Shanea Davis, VP, Real Estate, Property & Asset Management
Chad Ballentine, VP, Demand Response and Innovative Mobility
Brian Carter, VP, Marketing and Communications
Gardner Tabon, VP, Safety, Risk Management, and Accessible Services
Muhammad Abdullah, Senior Director, Chief Procurement & Compliance Officer
Susan Renshaw, Controller
Steven Salinas, Director of Network Security
David Newton, IT Service Delivery Manager
Lori Hyde, Program Manager IV, Network Cybersecurity

# Table of Contents

# EXECUTIVE SUMMARY

As part of our Fiscal Year 2020 Internal Audit Plan approved by the Capital Metro Board, we performed an audit of the IT Endpoint Management process to determine the effectiveness of internal controls over patching and machine configuration. The audit results including the objective, scope, and conclusion are as follows.

## Background

The IT Department has established policies, procedures and configuration standards to help protect the confidentiality, integrity and availability of Capital Metro systems. This includes a defense in depth approach which starts with the security and configuration of all endpoints connected to the network and employee training. Endpoint is a generic term that covers all devices on the network which includes the following: servers, laptop and desktop PC's, tablets, TVM's, printers, etc. Capital Metro has more than 1,000 endpoints connected to its network and the timely patching and monitoring of these devices is critical to the security of the overall network.

Various software tools have been deployed by Capital Metro to protect and monitor the performance of the endpoints on the network. This includes anti-virus software as well as network monitoring and patch management software to ensure all endpoints have current software updates and are protected from known malware vulnerabilities. In the software industry, program updates are usually released once a week by software companies in what is referred to as "Patch Tuesday". Endpoint security management is a software approach which helps to identify and manage the users' computer and data access over a corporate network, in order to maintain and comply with the organization's policies and standards. The IT Department has developed an IT Practices & Procedures Manual which defines the controls (e.g. patch management, virus protection, change controls, etc.) that help ensure the confidentiality, integrity and availability of Capital Metro systems.

## Audit Objective & Scope

The primary objective of this audit was to determine whether the design and operating effectiveness of internal controls over patching and machine configuration is sufficient to address the risks. The scope included a review of all endpoints connected to the network, conducting interviews, reviewing Authority policies/procedures, applicable contracts, and data analytics on the following four systems: Microsoft SCCM; Antivirus Software; ServiceNow CMDB; and Microsoft Active Directory.

## Opinion

Internal controls related to patching and machine configuration are generally in place and properly functioning. During our review we identified internal controls that require improvement and made the following recommendations:

1. Explore Enhanced System Software Solutions
2. Update IT Policies & Procedures
3. Leverage Data Analytics Across Endpoint Management Tools
4. Define Patching Timelines by Patch Severity Rating

More details regarding issue/risk and recommendation can be found in the detailed audit report below.

This audit was conducted in accordance with the U.S. Government Accountability Office's Generally Accepted Government Auditing Standards (GAGAS) and the Institute of Internal Auditor's International Professional Practices Framework (IPPF). 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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. The audit was conducted by the following staff members in the Capital Metro Internal Audit Department:

- UT Audit Interns
- Terry Follmer, VP of Internal Audit (Project Lead)

Recommendations to strengthen controls and improve accountability were provided to management. Management agrees with the internal audit recommendations and has provided target completion dates which are included in the detailed audit report below. A follow-up audit is performed semi-annually (i.e. May and November) to ensure management action plans for all issued audit reports are completed timely.

We appreciate the cooperation and assistance provided to us throughout this audit.

| *Issues & Risk* | *Recommendation* | *Management Action Plan* |
|---|---|---|
| **1. <u>EXPLORE ENHANCED SYSTEM MANAGEMENT SOFTWARE SOLUTIONS</u>**<br><br>Capital Metro has been using the Microsoft System Center Configuration Manager (SCCM), which is a software management suite that allows users to manage a large number of Windows based computers. SCCM features remote control, patch management, operating system deployment, network protection and other various services. While this tool is effective at deploying Microsoft patches, we noted that the tools has limitations in the following areas: ability to identify the patch severity rating (i.e. Critical, High, Medium, Low) of the missing patches; manage Mac iOS and related patches; and does not have "relay management" capability. Capital Metro has more than 1,000 devices on the network and tools like IBM BigFix can handle all of these shortcomings and will result efficiencies within the IT Department thus freeing up their time to perform more value added functions in the place of the manual monitoring and patching. | The Director of Network Services should explore on a cost-benefit basis other system management software solutions (e.g. IBM BigFix, etc.) that will enable the identification and deployment of patches based upon severity rating as well as improved capabilities on non-Microsoft operating systems (e.g. UNIX, Mac iOS, etc.). | Management agrees and has developed the action plan below.<br><br>**<u>Target Completion Date</u>**: 7/31/2020<br><br>IT has already budgeted for and is in the process of implementing a solution for the MacOS (JAMF) that is not manual. While there is a plethora of system management solutions available on the market, Microsoft SCCM is included with the Capital Metro Enterprise agreement and does not cost the agency any additional funds. Also, the staff has all been trained on MS SCCM. The technical solution in place will always depend on the amount of manpower necessary to maintain the system and that is the primary factor in managing these systems. Patch severity is evaluated by the team and tagged in the SCCM system for application to the workstations at this time and is reviewed on a regular basis for compliance. |

| *Issues & Risk* | *Recommendation* | *Management Action Plan* |
|---|---|---|
| **2. <u>UPDATE IT POLICIES & PROCEDURES</u>**<br><br>The IT Department has an IT Practices and Procedures Manual that covers many IT administration and security areas (e.g. governance, virus protections, data management, encryption, etc.). We noted that the manual is in the process of being updated and during Dell Secureworks 2019 security review they identified five policies as missing and provided Capital Metro with rough policy drafts as follows: Cybersecurity Program Policy; Acceptable Use Standard; Business Continuity and Disaster Recovery Policy; SDLC and Project Management Policy; and Security Awareness and Training Policy. We believe updating the department policies and procedures and incorporating the feedback from Dell Secureworks will further strengthen IT Endpoint Management controls. | The Director of Network Services to complete the updates to IT policies and procedures. | Management agrees and has developed the action plan below.<br><br>**<u>Target Completion Date</u>**: 8/31/2020<br><br>IT has the following policies in place that partially or entirely cover the recommendations:<br><br>IT Security Response Procedure and a Cyber security roadmap. We will work to consolidate existing documentation and practices into a comprehensive cyber security program policy.<br><br>There is an existing Technology Use policy IT-201 in place and is reviewed on an annual basis.<br><br>There is an existing Continuity of Operations policy and procedure in place.<br><br>There is existing SDLC documentation. Steven will work with the enterprise application team to consolidate a comprehensive document to address this request.<br><br>There is an existing mandatory end user security awareness training program in place. IT can develop formal documentation to support that on-going effort. |

| *Issues & Risk* | *Recommendation* | *Management Action Plan* |
|---|---|---|
| **3. <u>LEVERAGE DATA ANALYTICS ACROSS ENDPOINT MANAGEMENT TOOLS</u>**<br>The IT security industry has not developed a comprehensive endpoint management tool, therefore organizations must manage/monitor IT endpoint security using a variety of software tools that don't always share data openly across the software tools. As a result, most organization have manually built their own comprehensive endpoint management database by aggregating the key endpoint data from the endpoint management security tools that have been deployed. Capital Metro primarily uses the following endpoint management tools: Microsoft SCCM; Antivirus Software; ServiceNow CMDB; and Microsoft Active Directory.<br><br>During our audit, the UT Audit Interns created a comprehensive database consolidating endpoint data from these four systems, and using the Microsoft Power Query tool they were able to identify the highest risk machines on the network. This new tool allows for the aggregation of all known endpoint attributes (e.g. User/Machine name, IP/MAC address, Operating System; Antivirus Software version; patching history; last login date; etc.). This analysis help ensure all endpoint are up to date and exceptions can be quickly identified and remediated. | The Director of Network Services should carryforward the Microsoft Power Query data analytics tool, and run the analysis on at least a quarterly basis to identify the highest risk machines. The highest risk machines should be identified, located and remediated on at least a quarterly basis. | Management agrees and has developed the action plan below.<br><br>**<u>Target Completion Date</u>**: 7/31/2020<br><br>IT will have our Cyber Security Program Manager assess the solution and provide recommendations to continue its use or leverage other tools in the pipeline to maximize this effort. The limitation is one of priority and resources to address. |

| *Issues & Risk* | *Recommendation* | *Management Action Plan* |
|---|---|---|
| **4. <u>DEFINE PATCHING TIMELINES BY PATCH SEVERITY RATING</u>**<br><br>The software industry typically releases patch updates weekly, and as part of the release they rate the severity of patches using the following severity rating system: Critical; High; Medium; and Low. Critical patches are defined by Microsoft as "a vulnerability whose exploitation could allow code execution without user interaction". A best practice is to specifically define a tiered software patch implementation timeline based upon the patch's severity rating. Most organization have chosen a 14 to 30-day timeline from patch release date to install "critical" patches. Capital Metro's IT Practice & Procedures manual does not specifically define patch implementation deadlines and instead states "patches should be installed within 60 days or as directed by vendor" (IT Practices & Procedures Manual section 10.4). | The Director of Network Services will further define patch management standards based upon the manufacturer's severity rating standards (e.g. Critical; High; Medium; and Low) and clearly state the maximum number of elapsed days from the patch release date for installation. The IT Department will measure compliance with the patch management standards at least quarterly, and machines out of tolerance will be identified and remediated. | Management agrees and has developed the action plan below.<br><br>**<u>Target Completion Date</u>**: 5/31/2020<br><br>Patch Management is currently done on a monthly basis in accordance with the formal Microsoft schedule. Any ad hoc critical patches are addressed as soon as possible after appropriate testing to ensure they do not adversely affect our applications, many of which are dated or developed in house. |