Audit Team

Brenda Berlin, CPA, IT Audit Supervisor
Jared Miller, CFE, CISA, Audit Supervisor
Nicholas Jimroglou, CISA, Lead IT Auditor
Karin Doughty, CISA, Lead IT Auditor
Brian Cheli, CISSP, CISA, Senior IT Auditor
Joe Ebiziem, CISA, Senior IT Auditor

Audit Management

Timothy M. O’Brien, CPA, Auditor
Valerie Walling, CPA, Deputy Auditor
Dawn Wiseman, CRMA, Audit Director
Kevin Sear, CPA, CIA, CISA, CFE, CGMA, Audit Director

Audit Committee

Timothy M. O’Brien, CPA, Chairman
Rudolfo Payan, Vice Chairman
Jack Blumenthal
Leslie Mitchell
Florine Nath
Charles Scheibe
Ed Scholz

You can obtain copies of this report by contacting us:

Office of the Auditor
201 West Colfax Avenue, #705
Denver CO, 80202
(720) 913-5000  ♦  Fax (720) 913-5253

Or download and view an electronic copy by visiting our website at: www.denverauditor.org.

Cover illustration by Denver Auditor’s Office staff.
May 28, 2020

AUDITOR’S LETTER

The objective of our audit was to evaluate the patch management program for the City and County of Denver’s information technology systems. This audit found some areas of strength and some areas that need improvement. Because of the information security sensitivities involved with patch management, these issues have been communicated separately to the relevant city agencies for their remediation.

This audit is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, “General Powers and Duties of Auditor.” We conducted this performance audit in accordance with generally accepted government auditing standards. Those 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We extend our appreciation to the personnel in the relevant city agencies who assisted and cooperated with us during the audit. For any questions, please feel free to contact me at 720-913-5000.

Denver Auditor’s Office

Timothy M. O’Brien, CPA
Auditor
BACKGROUND

What Is Patch Management?
Cyber criminals constantly try to hack into vulnerable information technology systems and hardware to gain unauthorized access to data. Usually technology vendors thoroughly test their systems for cybersecurity vulnerabilities; however, hackers are coming up with new ways to exploit systems.

To combat vulnerabilities, vendors develop corrections or fixes for security loopholes or flaws as those become known. These corrections or fixes are applied to systems through “patches.” Patches are very common. According to the SysAdmin Audit Network and Security, or SANS, Institute, a security research and education company: “In the software world, rarely, if ever, is an application developed without having the need to be corrected, upgraded, or modified.”

Cybersecurity is not the only reason to apply patches to a system. In some cases, a patch adds new features. For example, a recent software update (i.e., patch) for the iPhone added a variety of new features including dark mode, a photos tab, and enhancements to portrait lighting when taking a photo.

“Patch management” is the process of identifying, acquiring, installing, and verifying patches for information technology systems. There are many models of what an effective patch management program should look like, but all have certain common characteristics.

Elements of an Effective Policy and Procedure

According to the SANS Institute, an effective patch management policy should, at a minimum, clearly define the program objectives and describe the scope of what should be patched, the roles and responsibilities of staff, and the minimum standards for compliance.

A procedure should contain the details of a patch management process, such as when and how to identify the systems to be patched, identify the patches available, develop an installation plan, and install patches.

---

4 Ibid.
Figure 1 above demonstrates a typical patch management cycle.

- **Identifying the Systems to be Patched** – Establishing a complete and accurate inventory of information technology systems is a key component of an effective patch management program. Without knowing the systems managed, it is impossible to know what needs to be patched.

  According to the SANS Institute, asset inventory management is an "essential prerequisite for patch and vulnerability management. Before a computer system is accredited or initially commissioned into production, an inventory of software assets installed should be taken. This inventory should be regularly updated."^6^  

- **Identifying the Patches Available** – Centralized information technology scanning tools are the most commonly used method for identifying when and what patches are available. These tools can report on vulnerabilities identified in the information system environment and whether a patch is available to fix the problem.

  Vendors usually classify patches by importance. For example, a “critical” patch is one that a vendor recommends installing immediately because it fixes a vulnerability such as susceptibility to malware. In contrast, a patch classified as "low" is one that has minimal impact on a system and that organizations should evaluate as to whether they want to install.

  Some vendors have established a standard timeline for when patches become available. For example, Microsoft deploys most of

---

^6^ Ibid.
its patches on the second Tuesday of each month.\textsuperscript{7}

- **Developing an Installation Plan** – An installation plan should include details on testing the patch, when it should be installed with consideration to minimizing downtime, how to communicate the installation, and what to do if the patch either does not work or has a negative impact on the system and has to be uninstalled (i.e., a “back out” plan).

A thorough installation plan is necessary for many reasons. For example, patches are often applied to the city’s critical systems, and they could have a significant negative impact on city staff and residents if a system is rendered unavailable and stops working properly. In addition, patches are sometimes not compatible with existing hardware or software, so installing the patch could lead to other problems. In some cases, it is necessary to weigh the risks and rewards of applying a patch.

- **Installing a Patch** – After a patch is tested and approved, a system administrator can install the patch to the appropriate systems. System administrators can use automated tools to install patches, which is especially useful when managing large information technology environments. It is important to communicate with system users after a patch has been installed to ensure the system continues to function normally. If the system is not functioning properly, the patch may have to be uninstalled through the “back out” plan.

### Why Patch Management Is Important

An effective patch management process helps reduce cybersecurity risks across information technology systems. Installing patches in a timely manner can lessen the chance of a breach and any resulting data loss. According to the Ponemon Institute, an independent research firm on data protection and emerging information technologies, “60% of cyberattack victims report that their breaches could have been prevented by installing an available patch.”\textsuperscript{8}

Some of the largest data breaches reported recently have been because of unpatched systems. These include data breaches at Equifax, JP Morgan Chase, Target, The Home Depot, and Marriott.\textsuperscript{9} Millions of customers were impacted in these cases, which resulted in lawsuits, fines, and reputational damage to the companies.


In addition, the Institute of Internal Auditors, an organization established to provide leadership for the internal auditing profession, advises that organizations with good patch management:

- “Spend less money and [information technology] energy on unplanned work”;
- “Spend more money and [information technology] energy on new work and achieving business goals”;
- “Experience less downtime”;
- “Install patches with minimum disruption”; and

The lack of an effective patch management process can be costly. The average cost of a data breach in 2019 was over $8 million.\footnote{“Cost of a Data Breach Report” (2019), IBM Security, accessed Jan. 24, 2020, https://databreachcalculator.mybluemix.net.}

Poor patch management processes can cost organizations in other ways also. For example, the Institute of Internal Auditors states that poor change management processes can cause:

- “Attrition of highly qualified [information technology] staff due to frustration over low-quality results”;
- “Poor quality systems that make employees ineffective and inefficient or that alienate customers”; and
- “Missed opportunities to provide innovative or more efficient products and services to customers.”\footnote{The Institute of Internal Auditors, "Change and Patch Management Controls: Critical for Organizational Success" (2012), accessed Jan. 23, 2020, https://chapters.theiia.org/montreal/ChapterDocuments/GTAG%202%20-%20Change%20and%20Patch%20Management%20Controls%20Critical%20for%20Organizational%20Success%202nd%20ed.pdf.}

This audit found some areas of strength in the City and County of Denver's patch management program as well as some areas that need improvement.
Office of the Auditor

The Auditor of the City and County of Denver is independently elected by the citizens of Denver. He is responsible for examining and evaluating the operations of City agencies and contractors for the purpose of ensuring the proper and efficient use of City resources. He also provides other audit services and information to City Council, the Mayor, and the public to improve all aspects of Denver's government.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities regarding the integrity of the City's finances and operations, including the reliability of the City's financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of City operations, thereby enhancing citizen confidence and avoiding any appearance of a conflict of interest.

Our Mission

We deliver independent, transparent, and professional oversight in order to safeguard and improve the public's investment in the City of Denver. Our work is performed on behalf of everyone who cares about the City, including its residents, workers, and decision-makers.