FOLLOW-UP REPORT

Multi-Agency

Patch Management

JANUARY 2022

TIMOTHY M. O'BRIEN, CPA
DENVER AUDITOR

OFFICE OF THE AUDITOR
AUDIT SERVICES DIVISION, CITY AND COUNTY OF DENVER

Audit Team

Jared Miller, CFE, CISA, CDPSE, Information Systems Audit Manager
Nicholas Jimroglou, CISA, CDPSE, Information Systems Audit Lead
Karin Doughty, CISA, CDPSE, Information Systems Audit Lead
Daniel Emirkhanian, MPA, Associate Auditor

Audit Management

Timothy M. O'Brien, CPA, Auditor
Valerie Walling, CPA, Deputy Auditor
Dawn Wiseman, CRMA, 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.

City and County of Denver

TIMOTHY M. O'BRIEN, CPA
AUDITOR

201 West Colfax Avenue, #705, Denver, Colorado 80202
(720) 913-5000 | Fax (720) 913-5253 | www.denverauditor.org

AUDITOR'S LETTER

January 6, 2022

In keeping with generally accepted government auditing standards and Auditor's Office policy, as authorized by city ordinance, the Audit Services Division has a responsibility to monitor and follow up on audit recommendations to ensure city agencies address audit findings through appropriate corrective action and to aid us in planning future audits.

In our follow-up effort for the "Patch Management" audit report issued in May 2020, we 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. However, we include background information in this report as a reference.

I would like to express our sincere appreciation to the personnel in the relevant city agencies who assisted us throughout the audit and the follow-up process. 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 common. According to the SysAdmin Audit Network and Security Institute, SANS, 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."[1]

Cybersecurity is not the only reason to apply patches to a system. In some cases, a patch adds new features. For example, a 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.[2]

"Patch management" is the process of identifying, acquiring, installing, and verifying patches for information technology systems.[3] There are many models of what an effective patch management program should look like, but all have certain common characteristics.[4]

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."[5]

Some of the largest data breaches reported in recent years have been

[1] Brad Ruppert, SANS Institute, "Patch Management" (February 2007), accessed Jan. 23, 2020, https://www.sans.org/reading-room/whitepapers/iso17799/patch-management-2064.

[2] "New Features Available with iOS 13," Apple Inc., accessed Jan. 23, 2020, https://www.apple.com/ios/ios-13/features/.

[3] National Institute of Standards and Technology, Special Publication 800-40 (Revision 3), "Guide to Enterprise Patch Management Technologies," (2013), accessed Jan. 31, 2020, https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final.

[4] National Institute of Standards and Technology, Special Publication 800-40 (Revision 3).

[5] "Costs and Consequences of Gaps in Vulnerability Response," Ponemon Institute LLC, accessed Jan. 24, 2020, https://www.servicenow.com/content/dam/servicenow-assets/public/en-us/doc-type/resource-center/analyst-report/ponemon-state-of-vulnerability-response.pdf.

because of unpatched systems. These include data breaches at Equifax, JP Morgan Chase, Target, The Home Depot, and Marriott.[6] 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."
- "Focus more on improvements and less on 'putting out fires."[7]

The lack of an effective patch management process can be costly. The average cost of a data breach in 2019 was over $8 million.[8]

Poor patch management processes can cost organizations in other ways also. For example, The Institute of Internal Auditors says 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."
- "Missed opportunities to provide innovative or more efficient products and services to customers."[9]

[6] Mandy Fisher, "10 Biggest Security Breaches from Unpatched Software," 1E, Feb. 8, 2019, accessed Jan. 24, 2020, https://www.1e.com/news-insights/blogs/10-unpatched-software-security-breaches/.

[7] 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%20 Controls%20Critical%20for%20Organizational%20Success_2nd%20ed.pdf.

[8] "Cost of a Data Breach Report" (2019), IBM Security, accessed Jan. 24, 2020, https://databreachcalculator.mybluemix.net.

[9] 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%20 Controls%20Critical%20for%20Organizational%20Success_2nd%20ed.pdf.

Office of the Auditor

The **Auditor** of the City and County of Denver is independently elected by the residents 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 residents' confidence and avoiding any appearance of a conflict of interest.

201 West Colfax Avenue #705

Denver CO, 80202

(720) 913-5000 | Fax (720) 913-5253

www.denverauditor.org

Our Mission

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