AUDIT REPORT
Patch Management
Information Technology
June 2022

Internal Audit Department

City of Fort Smith, Arkansas

Tracey Shockley, CFE, CCA

Internal Audit Director

Our Mission

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

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 continually trying to come up with new ways to exploit systems.

Vendors develop corrections or fixes for security loopholes or flaws as those become known in order to combat vulnerabilities. Corrections or fixes are applied to systems through "patches" that are provided free of charge to licensees by the software vendor. According to the Sys Admin 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."

Patches can add new features and so Cybersecurity is not the only reason to apply patches to a system. For example, a recent software update (i.e., patch) for a brand of cell phone that added a variety of new features including dark mode, a photos tab, and enhancements to portrait lighting when taking a photo.

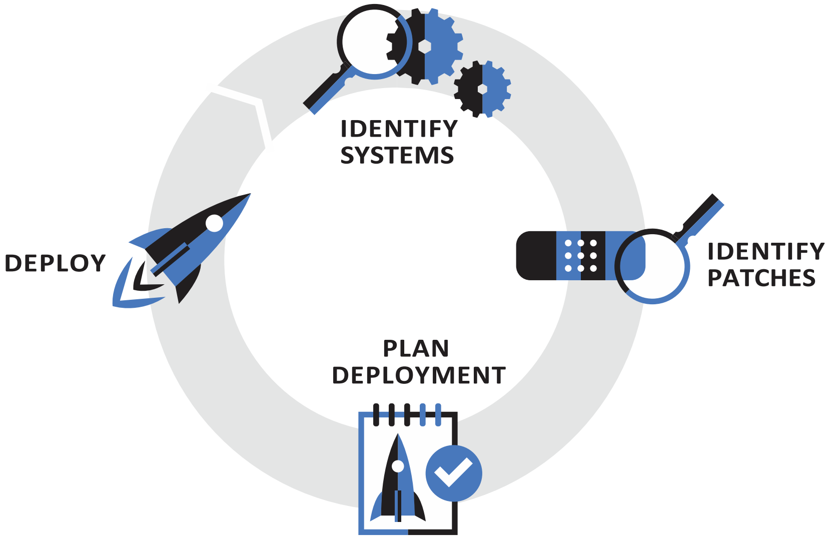
"Patch management" is the process of identifying, acquiring, installing, and verifying patches for information technology systems. There are many models of what an effective patch management program should look like, but all have certain common characteristics.

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, develop an installation plan, and install patches.

FIGURE 1. Example of a Patch Management Process



Source: Image designed by Auditor's Office.

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."[1]

- **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, there are companies who deploy most of its patches on specific day of each month.

[1] Ibid.

- **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.

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.[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
- “Focus more on improvements and less on ‘putting out fires.’”[2]

The lack of an effective patch management process can be costly. The average cost of a data breach in 2019 was over $8 million.[3]

[2] 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_2nd%20ed.pdf.

[3] “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."[4]

Conclusion

The objective of our audit was to evaluate the patch management process for the City's information technology system. The City Administrator and the Interim ITS Department Head did not assist in provide any information regarding the City's patch management policies, procedures or practices despite numerous requests from Internal Audit for this information. Additionally, the Interim ITS Department Head would not respond to meeting request or emails from Internal Audit.

This audit found some areas that need improvement in the City's patch management program based upon the limited amount of information received from inquiries. ITS does not have a capable work order system that could track job time spent on such tasks as operations and maintenance, deployments, projects and planned work. This system would also be able to track parts, materials, resources, contracted labor, etc... Additionally, because of the information security sensitivities involved with patch management, additional information has been communicated separately so that the Information Technology Department can address the items identified. The recommendations are based upon current knowledge IA was able to obtain during the limited audit.

[4] 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_2nd%20ed.pdf.