FEATURE

Patch Management Risks

Prepare to continuously audit

By Daniel T. Yunker and John Norenberg

Among the many responsibilities of healthcare internal audit and compliance professionals is verifying that their organization's information technology (IT) systems are up to date for privacy and security regulation compliance. While patch management has not historically been on the radar for internal audit and compliance teams, patch management is quickly becoming one of the most important controls to be monitored.

Since the dawn of enterprise computing in the 1960s, computer systems have gotten exponentially more complicated. Every generation of information systems builds on its predecessors, which has brought about the seeming magic of technology and its positive effects to our everyday lives. The downside to this growth is that no one person or small group can possibly understand every one of the trillions of lines of code, written by millions of developers, and used by billions of people.

Therefore, no one is surprised when unanticipated problems are exhibited in any computer system running in a live environment. Causes of problems range from user error and intersystem reactions to designer and developer error. As a result, developers issue fixes, often referred to as *patches*, to rectify these problems.

Given the sheer number of hardware and software systems in a typical enterprise environment, each with a vendor issuing patches to its systems, managing this maintenance activity requires a special focus by the IT team. The practice of identifying and deploying software updates is referred to as *patch management* and is considered one of the most important controls for managing an IT department.

All IT-related compliance and risk management functions seek to ensure that the IT systems are running properly. If the systems are not patched properly, they may not be running within the operating parameters for which they were initially purchased. Therefore, building programs for patch management and its assurance should be a cornerstone of any healthcare organization's IT, compliance and risk management operations.

Types of patches

Just as a wide variety of systems make up an enterprise's technological environment, a variety of patch types exist. Each type is important and needs to be considered in a comprehensive patch management policy and procedure set.

Security

The actions of cybercriminals attempting to gain access to personal information, including protected health information, are well known. Cybercriminals have become experts at breaking down enterprise systems and exploiting the openings that these code issues represent. Security patching is so important that an entire industry of hardware and software vendors has grown to help find, communicate, and distribute these security fixes. Arguably, because of the inherent criminal risk, security patches are the most important patch type.

Application process integrity

Application software issues can produce errant results. While security patches get a majority of attention, application

Patching identifies and deploys software updates to improve security and performance.

Systems and patch types need prioritization should time constraints or technical conflicts arise.

problems cannot be ignored. A computing error can mean the difference between the right and wrong dose of a medication in the healthcare setting, with similarly serious results in all industries. For this reason, application process integrity also should be considered a very important part of a patch management program.

Infrastructure process integrity

Computing infrastructure comprises all the hardware that runs the network, hardware in the data center, and some specialty software that allows the applications to operate. Every piece of infrastructure is loaded with software, whether it is hardware with embedded programming or actual software that drives the infrastructure, such as operating systems and database systems.

While each of these systems might be, and often is, patched for security or application process integrity, another large set of patches affects how the infrastructure systems run. Keeping these IT assets running at peak performance demands that these patches be applied periodically.

Patch management policies

With all the software being updated both at regular intervals and on an emergency basis, the patch status of systems may not be tracked accurately. A patch management policy is required, and adherence to the policy is crucial. The IT team is a primary stakeholder in this effort and should be involved in all steps.

Two schools of thought exist regarding patch management policies. Both come with upsides and downsides.

Limited scope

The first school of thought is that the policy should reflect the capabilities of the IT team and no more. Given the vast number of systems, including those that are not owned or managed by the IT department, one can understand why this method is attractive. A limited scope policy focuses on what the IT department can perform with high quality. A limited scope policy feels less ponderous to implement.

One problem with this method is that systems are frequently added that can lead to gaps in the patch management coverage. Another problem is that many systems are not owned or managed by the IT department. In provider healthcare, biomedical device management and human resources systems are common examples.

In addition, many cloud and vendor-managed systems, including the vendor relationships, are not owned by the IT department. In each of the areas, another policy must be created to manage those systems and relationships. Additionally, because of the rapid change, more policies need to be written to manage the content of the original policies, leading to policy sprawl.

Holistic scope

The second philosophy regarding patch management policies is holistic. The philosophy requires that all systems be listed, in some cases including personal devices, and categorized. Once the list is complete, details are added to each category with specific information about how different types of patches should be managed.

A holistic policy, being more general and inclusive, will lead to a smaller number of actual policies being written. But a holistic policy might be more difficult to administer and audit because it will require some level of interpretation.

When considering the two extremes of policy philosophy, keep in mind that no single right answer exists. A middle position can be acceptable that has a general policy governing all systems and specific policies to cover those systems for which patch management is mission critical.

Policy set components

Regardless of how a healthcare organization chooses to write its policies, certain pieces of information must be included in the policies and kept up to date:

1. A list of the systems and software that will require patching
2. Prioritization of the systems and patch types to take precedence should time constraints or technical conflicts arise
3. For each system and patch type, the timing of patches to be tested and applied to the systems
4. For each system and patch type, the designated owner of the patching process
5. A provision for focused testing and immediate implementation for emergency patches
6. A provision for managing systems for which patching is precluded, typically because of software vendor requirements
7. Reporting on the patch status of all systems on a regular basis

Lastly, and very importantly, the policy should recognize that, despite best efforts, some patches create more troubles than they solve. For these cases, the process to roll back or uninstall the patch needs to be included.

When building the policies, consider the various stakeholders who are affected by the patching process. The most obvious stakeholder is the IT group. Indeed, in many cases the policies are owned by one of the IT leaders.

However, the members of the user community are often forgotten. Because the application of patches typically requires the computer systems to be taken offline, certain users must have input regarding the timing in order to minimize business impact.

For example, consider a large hospital environment where one might assume that the best time to take clinical systems offline is at midnight on a Saturday night. However, that time might be the worst time for the emergency department. Find leadership to identify and help resolve these conflicts to ensure the success of the patch management policy.

Patch management auditing reimagined

The complexity of patch management, given all the systems involved, the vendors and the differences in their delivery methods, and the varying seriousness of the individual fixes, can make meaningful assessment and assurance difficult. Historically, a patch management audit consisted of a policy review, if policies existed, combined with a test of a sample of servers and workstations to determine compliance with the policies or at least the currency of their security-class patches.

The audits of the past have become less effective as complexity has increased. Rather than despair, consider that the same forces that created the problem—the systems themselves—can be part of the solution. The new approach requires an accurate inventory of the systems and their software and an equally accurate list of the patches from each vendor that are required for each device and system.

Then, you can easily imagine a system where each machine can be queried to see which patches are applied. The responses from every machine can then be used with analytic tools to perform an evidence-based review of the patch status of the entire network.

Taking this concept a step further, the environment might be upgraded so that rather than responding to queries, the machines themselves check their patch status against the master list and automatically report back their status. The last step will be to have the machines report their status in as close to real time as possible, including for outlier systems.

This level of continuous auditing would allow an organization to nearly fully ensure that systems are protected from the threats of cybercrime, application insecurity and infrastructure insecurity that are so common in today's environment.

Regulatory outlook

In addition to, and perhaps because of, the heightened risk posed by IT generally, and patch management specifically, standards are becoming stricter.

The U.S. Department of Defense (DOD) stated that enforcement of the Cybersecurity Maturity Model Certification (CMMC) will begin once rulemaking is complete to implement the program. All the DOD's contractors and subcontractors will have to comply with CMMC. The effect of this announcement is that the entire DOD supply chain will move from a check-the-box cyber attestation model to one

The patch status of all systems should be reported on a regular basis.

Technical capabilities have emerged to make continuous auditing more feasible.

that requires proof that the controls and policies are in place and that they are being followed.

The level of certification will be based on results attainment against National Institute of Standards and Technology (NIST) security controls (NIST SP 800-171 Rev. 2). Level one is a minimum for low strategic work. Level two is a transition step in cybersecurity maturity progression. Level three is a full demonstration of all controls in all circumstances and is required for all highly strategic programs, such as weapons systems.

Healthcare regulators, similar to regulators for all industries, are concerned about cybersecurity, so the cybersecurity requirements for healthcare are bound to become more stringent, perhaps moving to a CMMC-like model. Any new requirements would probably be enforced through the Health Insurance Portability and Accountability Act privacy regulations, Centers for Medicare & Medicaid Services reimbursement and the Office for Civil Rights.

Continuous auditing

Given growing risk, changing regulations and the sheer complexity of the modern computing environment, how do healthcare internal audit and compliance professionals proceed?

The answer lies in continuous auditing, which, as a concept, has been around for a while. Continuous auditing involves moving audit practices from testing a set of data once during a given period to testing all of the data as it is created, more or less in real time. For continuous auditing of patch management, every machine would be constantly reporting its patch status to the auditing system. If an unknown or otherwise improperly patched machine were to report in, the internal audit and IT teams could be dispatched to solve the problem.

Continuous auditing has not gained much traction due to a number of factors, including the very large technology requirements. Now, however, cost-effective technical capabilities have emerged to make continuous auditing of most aspects of IT controls a real possibility.

The good news is that the market is responding, with many vendors—both startups and large, established companies—signaling that they are developing the first generation of IT continuous auditing tools. Generally, these vendors highlight patch management as part of their initial product offerings. The prospect of needed tools is a welcome call to action for you to begin preparing for the new compliance requirements that are on the horizon.

Takeaways

1. IT systems must be kept up to date to keep them running efficiently, accurately and in compliance with privacy and security regulations.
2. Audits of patch management and providing assurance should be a cornerstone of an IT audit plan.
3. Adherence to sound patch management policies is just as important as creating them.
4. In developing patching policy, consider the various stakeholders that are affected.
5. The same forces that create the need for patching—the systems themselves—can also be part of the assurance solution.
6. The future state of continuous auditing might provide nearly complete assurance that systems are protected from common technology threats.

Summary

Patch management is increasingly vital to today's IT security, internal audit and compliance functions, and it must take a structured approach to compliance and assurance.

The first step is to make certain that patch management policies are in place and are not only appropriate but rooted in best practices. Your IT group is probably already patching their systems; however, without policy guidance, the group's processes might lead to an unforeseen failure.

The second step is to begin measuring against policies. Measurement can be, and has historically been, done using manual testing methods. However, manual methods increasingly are missing their assurance goals due to the size and complexity of what they are measuring. But one

must consider starting manually to perfect processes before continuous auditing is implemented. Manual methods also test the stability of the policies.

When continuous auditing tools become available, healthcare organizations should consider implementing them with the caveat that significant change in compliance operating workflows will be needed.

Lastly, as regulators move to a stricter cybersecurity assurance model, the complexity of the healthcare environment means that the implementation of these systems will take a considerable amount of time. But early adopters might expect to attain positive business and reputational results. Consider this article as a call to action. The time for organizations to create patch management policies and build their abilities around those policies in preparation for continuous auditing is now. **NP**

Daniel T. Yunker is a principal and healthcare internal audit leader in the healthcare risk consulting group at Crowe. He has an extensive background in leading healthcare organizations. Dan can be reached at Dan.Yunker@crowe.com and 312-899-1514.

John Norenberg is a senior manager in the healthcare risk consulting group at Crowe. He has previous experience as a senior healthcare IT executive leader in clinical operations, revenue cycle, population health, and IT strategy and infrastructure. John can be reached at John.Norenberg@crowe.com and 630-574-1634.