Ask the IT Auditor

Patch Management and Disaster Recovery

By Bill Daniels, Contributing Technology Committee Member

The AHIA Technology Committee hosts Tech Talk, a quarterly teleconference providing an opportunity for healthcare auditors to discuss technology-related topics. Questions to the "Ask the IT Auditor" column come from the AHIA Tech Talk session participants. The answers are a composite of the responses from the various IT auditors also on the calls. Tech Talk topics are often suggested in advance, but hot topics often arise during the teleconferences.

Dates for the quarterly Tech Talk calls are published on the AHIA website and communicated by email to AHIA members.

Patch management

How can an auditor verify patches, especially high-level security patches, have been successfully installed?

Many good products on the market can track patch releases and vulnerabilities. Some solutions can scan an IP range to search for known vulnerabilities. Many offerings include a portal to display a patching status score to help influence behaviors. The information can be particularly meaningful if the organization believes a patch was successfully applied but the vulnerability still exists. Many tools can be configured to look at various technical controls and report on patch status and configuration settings such as port settings, file sharing privileges and security log settings.

Some vendors may not allow the organization to apply software updates, patches or configuration changes. Laboratory and radiology systems are two examples. What are some solutions to address this risk?

Ideally, the contract between the organization and vendor will include language specifically addressing this concern. Regardless of contract terms, many vendors prohibit certain hardening approaches on their devices. Configuration changes, patches and even anti-virus software may not be permitted.

A common approach taken by some organizations to mitigate these risks is to segregate the systems on their network behind an additional firewall. If the less secure devices are compromised, the negative impact can be minimized because the devices are isolated.

What are good solutions for auditing desktop patch management?

As with servers, various solutions are available to deploy patches to desktops, laptops and other devices. Tools can recognize the base operating system (e.g. Windows, Linux, Mac) and monitor vulnerabilities. Some solutions employ a homogenous approach to patches by deploying the same patches to all devices with the same operating system. The approach looks at vulnerabilities at a point in time and provides a compliance check for each device.

Some tools require a client application to be loaded on a device which may require linking asset management and patch management processes. If a desktop is not included in the asset management records, it is possible the necessary client will not be installed and patches may not be applied.

The tool-based approach differs from a process-based approach although the two may complement one another. A process-based approach may help you better understand the lifecycle of the patching process:

1. Release date
2. Internal testing
3. Deployment schedule
4. Release to production devices
5. Confirmation and monitoring of applied patches and resolved vulnerabilities

What are some risks inherent in cloud-vendor patch strategies?

Some cloud-based service vendors are reluctant to commit to responsibility levels that many people believe HIPAA requires. Many vendors have chosen not to certify at a level that is expected by many healthcare entities.

The costs of cloud services may be favorable to the organization. The trade-off, however, may be lowered levels of compliance with expected security standards. Cloud-based solutions appeal to end users like employees and physicians because of the relative ease in accessing files from anywhere.

Healthcare IT departments, however, face great challenges in understanding the risks, controlling document flow, defining and monitoring appropriate access and securing organizational data. While the number of cloud-based offerings increases, understanding and managing the risks will remain a challenge.

Disaster recovery

What is considered a comprehensive disaster recovery test? Does it include core systems only?

The risk management strategy of an organization, in addition to business continuity efforts and funding, will

influence the disaster recovery plan. The systems that are assessed as organization-critical with high availability levels generally are the first to be restored by IT, tested by the organization and reviewed by internal auditors.

Business continuity procedures should be documented, regularly discussed with employees and readily available. This documentation can help minimize productivity and data loss risks and ensure effective operations while systems and data are restored following a disaster or interruption in IT operations.

A Business Impact Analysis (BIA) should be prepared and approved for each key system. The analysis should define the amount of downtime the business can withstand before operations are adversely affected, and a recovery time objective should be documented and agreed to by IT department management.

Disaster recovery plans should be developed to be consistent with the BIA. Auditors should be familiar with the technologies involved and the criticality of the systems and data to be restored. In addition, auditors should evaluate the 'tone at the top' culture for effective communications between operations and IT departments.

Understanding the dependencies between disparate systems is a key step in defining disaster recovery plans and executing them. IT personnel often view systems based on a specific platform or application rather than on a set of technologies that support a key business process.

An application may be restored, but the underlying database may have a different recovery timeframe. In addition, business personnel may not be aware of all the technologies supporting the business process and the related dependencies. Internal auditors may provide value by helping to identify interrelated systems and helping ensure IT and business leaders are communicating to align strategies.

One disaster recovery approach some organizations take is to restore critical systems and related data to a 'cold site.' In this scenario, all the equipment needed for recovery must be staged and configured before restoration efforts can begin. This approach is generally less expensive, but it also requires more time to restore full functionality to end users.

Other organizations use a 'warm' or 'hot' site in which needed hardware is partially or fully configured to match the organization's IT environment. These services are generally more expensive but can shorten the time for full recovery.

Two other situations may provide opportunities for IT to test its disaster recovery readiness and for internal audit to participate.

- *Scheduled maintenance* – Many organizations combine recovery tests during times of scheduled maintenance. Application issues, product licensing, system configurations, personnel availability and commitment to achieving recovery-time objectives are common process challenges for IT, and risk areas for internal audit to review.
- *Weather events* – Significant weather events such as heavy rains, snowstorms, tornadoes, etc. may directly affect IT operations and systems uptime. Operations, IT and internal audit personnel may consider leveraging these live events to test disaster recovery plans.

How does an organization address the risk of disaster recovery with ASP vendors?

The first place to start is with contractual language to manage expectations from the vendor. The contract terms can then be managed and audited. The organization's BIAs should also address the use of patient portals, supply chain, human resources and other ASP solutions supporting the business process.

Another option may be to contract with other vendors. If the primary ASP vendor has an extended service interruption, the backup vendor may be engaged so the organization can continue with its processes. The use of ASP vendors is an expanding area for many organizations, and internal auditors are realizing the audit challenges inherent in those relationships. **NP**