BY SAJAY RAI AND PHILIP CHUKWUMA EDITED BY STEVE MAR

AUDITING GOVERNANCE OF CRITICAL INFORMATION

Auditors need to know what critical data their organization is storing and who can access it.

By now most readers are familiar with the story of Edward Snowden leaking the existence of the U.S. National Security Agency's (NSA's) PRISM surveillance system to the media. To the NSA, that was critical information. PRISM was supposed to be "top secret," yet the NSA trusted such critical information to an outside contractor.

The NSA incident raises questions about whether organizations understand what their critical information is and who can access it. Each year, many internal audit departments develop their audit plans assuming that their organization can answer those questions. This is a bad assumption because some organizations are still struggling to appropriately assess the risks of critical information governance and management.

For internal auditors, a good starting point to understand the current state of their organization's information governance and management process is the related policies. These policies detail the organization's requirements for defining, creating, storing, accessing, using, and transmitting critical data, as well as making it available. Some organizations have done an excellent job of defining these policies, whereas others are still defining their requirements and may make only a portion of this information available to auditors.

What Information Is Critical?

Information is proliferated across an organization in many ways—through mobile devices, in the cloud, or via its own servers or a service providers' servers. Typically, an organization must sift through all this data to identify the critical information. Auditors could locate this information through a:

- **Risk assessment.** An effective risk assessment program enables an organization to identify the critical information and the risks associated with it.
- **Business impact analysis.** Performed during an organization's business continuity or disaster recovery planning, a business impact analysis identifies its critical information and recovery-time objectives.
- **Data classification.** Organizations that have implemented a data classification policy typically identify confidential information such as trade secrets.

Where Is It Stored?

Determining where the critical information resides can get technical for auditors because most of the information resides in databases, files, and folders. Auditors may need the IT department's help to identify these systems and learn how they store critical data. Moreover,

SEND ITAUDIT ARTICLE IDEAS to Steve Mar at steve_mar2003@msn.com this information could reside outside of the organization's IT environment through an outsourced entity or in the cloud. Auditors need to trace the critical information as it moves from within the organization to the outside world by:

- Checking with the data architect to understand the data dictionary, data models, and metadata definitions and verify where the critical information resides.
- Reviewing the third-party vendor agreements and contracts to see whether they detail the type of information that external parties can access.
- Asking the IT security group to provide details about information residing in identity and access management systems.

Who Has Access?

Auditors also need to find out who has access to the organization's critical information. They can look for several controls:

- Does the organization have a good process for adding new users and deleting terminated users (i.e., provisioning and deprovisioning)? Does the process have approvals from information owners?
- Are the access rights reviewed and updated periodically by information owners? Does the review process incorporate the extended enterprise (i.e., outsourcers, third-party vendors, and cloud solution providers).
- Are the accesses logged appropriately for later review?
- Are the access logs reviewed for inappropriate attempts?

Third-party providers are the weakest link in security controls for many organizations. Often, organizations put their own employees through rigorous security controls but have minimal controls over third-party contractors who have access to information.

How Is It Used?

The next step for internal auditors is understanding how the critical information is used across the organization's IT systems. Specifically, auditors need to know how data leaves the network and whether the information can be hacked. To find out, they should ask these questions about security controls:

- If the critical information is leaving the organization's network, does the organization know where it is going? Is a log kept of all critical information leaving the network?

TO COMMENT on this article, EMAIL the author at sajay.rai@theiia.org .

- Is critical data encrypted before it leaves the network?
- Does the organization comply with regulatory and privacy laws, such as those covering personal health information, when the critical information leaves the network?
- Can an external hacker access critical information? Does the organization have enough security controls, such as an intrusion detection system, to identify such a threat?

Is It Available?

Auditors should consider whether critical information is available when needed. The network and IT architects can provide auditors information about redundant technology that is in place to ensure the availability of data.

In addition, auditors should determine whether the organization is prepared to handle incidents where the technology fails or a human error causes the information to be unavailable. Specifically, auditors should focus on two areas: the disaster recovery and incident response plans.

Disaster recovery plans are written in case service is interrupted. Auditors should review these plans to see whether they are complete and up-to-date—the documentation of the plan matches with the technology in place—and the plan has been tested recently. Many organizations do not test their disaster recovery plans before they have a "live" incident.

The organization's incident response plan details its procedures and personnel for managing and resolving incidents. Whereas the disaster recovery plan addresses the availability of data from a technology perspective, the incident response plan addresses the availability from a process or people perspective.

Understanding Is Key

If internal audit has a good grasp of the organization's critical information governance and management, its annual audit plan may be more impactful and provide better assurance for that information. On the other hand, if this governance and management process is not well understood, the audit plans might cover only a subset of the intended audit scope and leave the organization with unanticipated risk. IA

SAJAY RAI, CPA, CISSP, CISM, *is the president and CEO of Securely Yours LLC in Bloomfield Hills, Mich.* **PHILIP CHUKWUMA, CISSP,** *is the chief technology officer of Securely Yours.*