

Five Identity Challenges Affecting Your Risk Posture

By Collin Perry, CISSP, CISA

Protecting information assets — and the business as a whole — requires a way to identify and assess risks and take the necessary steps to reduce risk to levels acceptable to the organization. Managing user access to sensitive applications and data should involve applying automated controls to the areas of greatest business risk. Unfortunately, far too many enterprises are using outdated, manual approaches that do not effectively address the five most common identity risks faced by most organizations:

1. Orphan Accounts

Orphan accounts are a direct result of failure to remove access privileges when workers terminate or transfer jobs. Last year's security incident at Cox Communications — where a terminated employee remotely shut down part of the company's telecommunications network account — illustrates the business risk represented by orphan accounts.

Despite defined processes for handling employee terminations and transfers, many companies still face tough challenges in trying to manage orphan accounts. In large organizations with frequent turnover, it can be extremely difficult to identify and revoke these accounts because there are thousands of employees and hundreds of applications involved. For that reason, orphan accounts are a frequent focus for IT auditors looking for security risks.

2. Entitlement Creep

Entitlement creep is a phenomenon that exposes organizations to unnecessary business risks every day. As workers gradually accrue access privileges over time through transfers, promotions, or simply through the normal course of business, they collect "entitlements" beyond what they actually need to do their job. When trying to manage to a philosophy of least amount of privilege, entitlement creep is the enemy.

The recent Société Générale case provides a woeful example of the devastation caused by entitlement creep. A "middle office" employee is transferred to the "front-office" or trading department, but his access entitlements remain unchanged. Taking his old system access rights to his new job allowed him to conduct rogue trades and circumvent risk management systems, eventually resulting in a multi-million dollar loss.

3. Shared and Generic Accounts

Ineffective oversight of "shared" or "generic" accounts is often flagged as a control weakness by IT auditors because they are typically managed using manual processes and are hard to audit due to their anonymous nature. Shared accounts can be grouped into two main types:

- » **Application accounts** — usernames and passwords that are used by IT and Engineering staff for application communications — tend to proliferate and often go unmanaged. These accounts present a high risk of exploitation because they are known to development

A former IT auditor and security consultant offers practical guidance for improving IT controls and compliance performance

and support staff and can be visible in plain text inside of scripts, configuration files, etc.

- » **Privileged user accounts** (e.g., UNIX root) represent higher-than-average risk because they are often shared among administrators and can provide broad and unrestricted access privileges. These are essentially the keys to the kingdom and should be managed closely.

4. Separation of Duty Violations

Separation-of-duty (SOD) policies are designed to prevent fraud by ensuring that no one person has excessive control over one or more critical business transactions. For example, a person should not be able to create a vendor and then enter a transaction to pay that vendor. Instead, processes and activities should be properly reviewed and separated in order to reduce business risks.

In practice, the real risk around SOD arises not from failure to document SOD policies; most companies have these type of rules captured in spreadsheets or a control grid. The real challenge arises from the complexity and effort required to enforce the policy across dozens or even hundreds of applications and systems. Performing the required level of policy checking manually is next to impossible, yet auditors look for evidence that SOD is enforced.

5. Contractors or Temporary Workers

Today's corporations rely more heavily upon contractors. And while these ar-



rangements provide businesses with a competitive edge, there are associated risks that, if not handled properly, can far outweigh the benefits.

Securing corporate assets from contractors and temporary workers can be challenging. These workers often have access to sensitive systems and data, but in many cases do not have their 'active' status tracked in an HR or centralized system the same way as permanent employees. Consequently, proper access control can be a difficult challenge.

SO, WHAT CAN YOU DO?

The good news for companies struggling with identity management is that a lot of progress has been made in improving visibility and automating compliance in the last few years. With the right tools and approach, it's now possible to improve compliance and audit performance while reducing overall compliance costs. Here are some practical ways to get started:

Get Centralized Visibility to Identity Data

Organizations need an enterprise-wide view of identity data, so they can effectively analyze risk, make informed decisions, and implement appropriate controls. In the same way that Business Intelligence applications can improve visibility to sales, marketing, and financial data, "Identity Intelligence" solutions can help organizations pinpoint problems, improve oversight, and more effectively meet compliance reporting requirements.

By centralizing and leveraging identity data from all applications in the organization, companies can drastically improve controls efficiency and effectiveness while addressing many large organization problems such as employee terminations, transfers and privileged access management.

Automate Access Certifications

Many organizations conduct quarterly or annual reviews or "certifications" of user access to meet compliance requirements.

Replacing manual methods with tools that automate access certifications can lower costs, reduce errors, and improve audit results. In addition, by reducing the time required to complete access certifications, automation tools enable organizations to respond more rapidly and effectively to inappropriate access and policy violations.

Automated access certifications can help reduce entitlement creep by flagging excess or inappropriate access and revoking unnecessary privileges. Certifications can enable non-IT business managers as well as technology owners to regularly review and approve high risk and privileged user accounts. Certifications can also be used to increase oversight over temporary workers by providing visibility to access held by users who are not permanent employees.

Automate Policy Enforcement

Once organizations centralize identity data across all applications, it becomes much easier to automate SOD and other policy enforcement. An automated management solution enables organizations to centrally define and proactively monitor for SOD policy violations across thousands of users and hundreds of applications. Using automation, companies can move from manual, incomplete or sporadic enforcement of SOD policy to more sustainable and reliable controls.

Policy automation can help organizations detect and enforce any type of access policy, not just SOD. For example, rules can be defined to restrict access according to geographic location, business unit, or permanent or contractor status. Many business and IT controls can be made easier to audit and more effective through automated policy.

Take a Role-based Approach

To minimize business risk, organizations need to ensure that workers have appropriate access to systems, applications, and data. It sounds simple, but the pro-

cess of tying low-level access privileges to higher-level business policies and job functions or business roles is an enormous challenge.

The growing convergence of business and IT in the compliance process is elevating the importance of role-based access control. Role management enables more effective business oversight by translating cryptic, technical access rights into logical groupings called roles. This higher-level business context enables business managers to make more accurate decisions about who should have access to what resources based on job function.

Take Time to Innovate

Before you continue to just "pedal faster" with your existing approach to managing IT controls, you may want to take a look at the new solutions available for automating the process and consider replacing current controls with automated, policy-driven ones. You can achieve big results in controls optimization and increased assurance, while eliminating costly and unreliable manual tasks.

Remember, however, that there is no "magic wand" solution to automating compliance and IT controls. It's not just about the technology. Collaboration is required across many organizational stakeholders, both business and technical, to address identity management risks. Putting in place effective policies and controls is essential. For effective and sustainable compliance, you need the balanced ingredients of people, process, and technology. ■

About SailPoint

SailPoint helps organizations reduce compliance costs, strengthen internal controls and manage risks associated with user access to enterprise resources. SailPoint Identity IQ™, a comprehensive identity governance solution, automates access certifications, enforces policy, monitors activity, and effectively manages the entire role lifecycle.

Learn more at www.sailpoint.com.

