

User Access-related Risk Management: Compliance Is Not Enough

The demands of regulatory compliance are among the factors driving IT and security managers within large organizations to improve their user access governance processes, but the issues are broader and deeper than any regulations – and more serious than many senior executives think. The recent scandal at Société Générale offers lessons that every Chief Risk Officer, Chief Information Officer and Chief Security Officer should learn.

Large organizations face an ever-growing body of regulations. At the same time, nearly every facet of their operations are now dependent on or supported by automated systems. As a result, risks related to unauthorized or inappropriate access can appear anywhere within an organization at any time and spread rapidly through the business. All it takes is a single person with the wrong access. Such events range from relatively minor policy and compliance violations to major operational failures with substantial financial, legal, and reputational consequences.

While user access-related risk cannot be entirely eliminated, it can be monitored, managed, and mitigated through a sound approach to governance. It is important to remember, however, that regulatory compliance is not enough to ensure that risk is being managed properly. A passing grade on a compliance audit is no guarantee that adequate controls and access governance procedures are in place. An enterprise's access control system can be in full compliance with all applicable regulations and still be vulnerable to serious, unacceptable business risks that could have been mitigated or eliminated with the proper controls.

It is equally important to bear in mind that fines and other penalties for compliance failure are not the entire sum of an organization's risk exposure when access controls are inadequate. The costs of a security breach or data loss can dwarf any regulatory sanctions. The immediate financial impact of misuse of access or a malicious act of "information vandalism" can be enormous, and the damage to an organization's public image can be crippling. Even in a secure and compliant environment, it is still possible to issue inappropriate access entitlements that can lead to mistakes resulting in a loss of corporate intellectual property or service interruptions to critical revenue generating systems.

In addition to viewing access control as a defensive tool, many enterprises have discovered that an effective system can also overcome certain types of operating inefficiencies, thereby creating a business advantage. For example, a good control system can enable an enterprise to extend access to employees, or contractors in remote locations in a way that leads to more efficient business transactions without incurring additional security or compliance risks.

What can happen when user access risk is overlooked

A stunning example of the potential impact of poor management of access-related risk is the recent scandal at Société Générale, where a junior trader risked an estimated \$75 billion on futures positions over the course of a year without the knowledge or approval of his superiors at the bank. By the time the rogue trades were discovered, Société Générale was faced with a loss of \$7.2 billion.

Although it is too early to make an accurate assessment of the causes, it is apparent that the Société Générale disaster could at least have been limited in scale had the bank adhered to a few principles of sound access governance:

- The use of role management when granting or changing a user's access would have prevented this trader from being able to "drag" access rights to information resources from their previous position that wasn't necessary in their new job role.
- A business unit manager or an immediate supervisor should have been accountable for recertifying the appropriateness of the traders' access to their job role on a regular basis.

- An automated access risk remediation system would have detected that someone with a front office job role had access privileges to back office systems which created a segregation of duties violation and flagged it for immediate intervention.

Consequences of this kind are encountered when organizations fail to recognize the risks inherent in providing user access to information systems and therefore fail to manage them thoroughly.

When does access-related risk become unacceptable?

The foundation of any access risk management initiative should be adherence to the principle of *least privileged access*: legitimate users should have no more access than the minimum required to do their jobs. Unacceptable access risks begin to appear when this principle is violated, and it is violated on a regular basis within many large enterprises.

Consider these findings from a recent Ponemon Institute survey¹ of experienced IT practitioners from U.S. business and governmental organizations:

- User access rights are poorly managed. Seventy-eight percent of respondents believe that individuals have too much access to information assets that are not pertinent to their job description.
- Policies are not regularly checked and enforced. Sixty-nine percent indicate that access policies within their organizations are either enforced poorly or not at all. Meanwhile, only 30% state that their organization makes sure user access policies are validated.
- Organizations are not able to keep pace with changes to users' roles and they face serious noncompliance and business risk as a result. Responses show that more than half (55%) describe their company's ability to grant access rights based on role and job function as poor or nonexistent, including 42% who report that it is not done at all.
- Senior management lacks understanding of the importance of access governance. Seventy-four percent of respondents believe that senior management does not view, or is unsure that, access governance is a strategic security and risk imperative.

The failure to enforce the rule of least privileged access often results from one of four causes:

Entitlement inertia is the failure to remove previously issued entitlements once they are no longer necessary or appropriate. It is not unusual, for example, for employees to accumulate unnecessary access privileges as they are promoted or transferred within an organization. A human resources administrator with access to confidential employee records who is transferred to Accounting should not retain access to HR systems. An IT manager who is transferred from being a system administrator to a development role should no longer have access to the production system he was administering. Some of these entitlements may become segregation-of-duties violations over time or represent other security risks. If an organization's termination procedures are lax, former employees may even retain some or all of their access entitlements after their employment has ended.

These are surprisingly common problems in large organizations, and they are natural consequences of the usual pressure on IT departments to provide access quickly when employees are transferred or promoted into positions that require new entitlements. In addition, many enterprises simply lack the capability to manage the constant change to user's business roles to ensure that their entitlements are appropriate for their new job responsibilities. Whatever the cause, organizations that do not certify access on a regular basis are most susceptible to "entitlement creep" and to prolonged exploitation by system intruders whose access, once established, goes unnoticed.

¹ 2008 National Survey on Access Governance, Ponemon Institute, February 2008

Compliance myopia results from the mistaken assumption that compliance with access-related regulatory guidelines ensures adequate access risk management. Just because access rights meet regulatory guidelines does not mean that they are consistent with the rule of least privileged access and other access governance best practices.

Regulatory compliance is prescriptive risk management. It calls out the areas of controls and the requirements for evidence of compliance. But its scope is limited to the business processes that the mandate was designed to govern. For example, SOX prescribes a set of controls for financial reporting but isn't concerned with data privacy regulatory requirements.

In addition, external auditors attest to the effectiveness of processes and controls and to the absence of compliance violations in whatever spot checks are made. A passed audit is not a guarantee that there are no unacceptable access-related risks. Consequently, focusing only on compliance can lead enterprises to overlook the issuance of unnecessary or otherwise inappropriate entitlements that, in turn, can cause trouble down the road in areas that are not covered by a regulation.

Rubber-stamping occurs when business managers are asked to review and approve access entitlements that are communicated to them in a security syntax language that they cannot understand. Asking business unit managers to certify employee access using a RACF mainframe security administrator's report is a typical scenario that external auditors fail organizations on. The business unit manager does not have the context to understand the user entitlements on a mainframe application unless the entitlements are presented in business friendly terms that relate to a user's job responsibilities. Pressed for time and with other responsibilities that may seem more important to them, managers may review and approve entitlements without truly understanding them.

Accountability loopholes are open as long as full responsibility for access governance is limited to IT. IT security teams are operationalizing access on the request of the business, but they do not have the business context to understand what level of access is needed for a particular job function or business responsibility. Business units and IT teams are certainly not experts in compliance regulations but audit and compliance departments are. It is essential, therefore, that audit, risk and compliance teams collaborate on managing access policies, and that accountability for compliance with regulations and policy be extended to the appropriate business managers.

Spreadsheet-based records of user access data can create accountability loopholes. They are labor-intensive, error-prone, and incapable of providing adequate audit trails and effective evidence of compliance. Spreadsheets also fail to drive accountability for governing user access as they aren't effective at automating the process of access authorization and review by business managers, who are ultimately responsible for authorizing and certifying the appropriateness of user access.

How access risk can materialize in the organization

Once access-related vulnerabilities appear within an enterprise information system, problems can materialize in several ways.

Inadvertent error can lead to data loss, operating failure, or other negative consequences. These events are the result of unintentional mistakes, but they can be just as costly as deliberate system attacks. For example, a software developer given unneeded access to an organization's production system could cause a system crash or other serious operating problems by testing software in the production environment. If the application or system is one that generates revenue, system availability issues can lead to a loss of revenue.

Because user access data resides in directories located in disparate systems, many organizations lack the ability to get a composite view of access across all information resources and all entitlements within those resources. If access is managed on a resource by resource (siloe) basis, the risk of creating a separation of duties compliance violation is relatively high because the mapping of entitlements between applications can't be seen.

Insider malfeasance is a surprisingly common occurrence. A survey conducted by McAfee in April 2007 was summarized as follows by Information Age:

60% of respondents said that system breaches were chiefly the work of individuals operating within the firewall – the staff, sub-contractors, partners and others that represent the so-called ‘insider threat’. This was not the most profound revelation, however. Participants in the research were also willing to point to the nature and intent of these insider-led leaks: although the majority of such incidents were judged to result from ignorance or negligence of security processes, in a murky 23% of cases the activity was deemed by respondents to be purely ‘malicious’.²

Société Générale’s \$7.2 billion loss was evidently the result of intentional access abuse by an employee, not an outsider. The bank’s vulnerability began with user access entitlements that should have been revoked when the employee was transferred to the trading department but were not.

Undetected security breaches are a constant threat to every large organization’s IT infrastructure. When an intruder successfully penetrates a system firewall and other “perimeter” defenses, the presence of this unauthorized user can and should be recognized instantly by internal access control and monitoring systems. Unfortunately, such breaches often go undetected as the result of an enterprise’s failure to follow basic access governance best practices, enabling intruders to establish and retain access to mission-critical applications and sensitive information for months or even years.

The well-known case of the TJX data breach—the total cost of which is now estimated by some to eventually reach more than \$500 million—began with malicious hacking into the company’s IT system by outsiders intent on stealing credit card data and other customer identity information. The hackers set up their own accounts within the TJX system, but the company did not detect them for nearly a year and a half – an indication that TJX lacked a proper system for reviewing and recertifying access in order to see orphaned accounts that could not be linked to a user and then delete them.

Once again, the Société Générale example is instructive. The rogue trader in that case created unauthorized and inappropriate accounts for himself that went undetected for lack of a regular and thorough review and recertification process.

Outsourcing can be another source of unintentional error. When a third party becomes involved in managing an enterprise’s information assets, there is an inherent increase in risk. This should be recognized and managed by ensuring that the third party conforms to all client enterprise security policies.

The consequences of unacceptable levels of risk

The actual costs that an enterprise can incur as a result of poor risk management stem from a variety of sources, but they generally fall into three broad risk categories.

Legal and regulatory risk can entail financial liabilities in the form of fines, restitution, and remediation costs.

Operational risk, due either to deliberate malfeasance or human error, can also lead to enormous costs resulting from lack of system availability or loss of revenue. According to the Ponemon Institute’s 2007 annual study of data breach costs in the US:

The cost of lost business continued to increase at more than 30 percent, averaging \$4.1 million or \$128 per record compromised. Lost business now accounts for 65 percent of data breach costs compared to 54 percent in the 2006 study.³

² Information Age, August 2007 http://www.information-age.com/article/2007/august_2007/inside_job

³ 2007 Annual Study: Cost of a Data Breach, Ponemon Institute

Brand and reputational risk associated with a loss of customer or investor confidence can, if realized, be costly as well. Financial institutions and any organization that does business with consumers are especially vulnerable. Also, a 2006 Ponemon study showed that customer churn rates due to a data breach of their information was as high as 7%.⁴

What to do about access-related risk

As noted earlier, the threshold for unacceptable levels of access-related risk is the rule of least privileged access. But this is just the beginning. It is essential to **monitor**, **manage** and **mitigate** access-related risk throughout the enterprise with a fully automated technology platform.

Most large enterprises already have a set of policies designed to ensure that proper oversight of system access is maintained. But in many cases, these policies have not been fully operationalized. As long as they reside in three-ring binders without being instantiated into daily operating practice and procedure, the policies are not likely to be enforced consistently. Automation is the key to driving comprehensive access risk management into the DNA of the enterprise.

An automated system must enable the organization to:

1. **Adopt the principle of least privileged access** to ensure that users have no more access than the minimum required to do their jobs.
2. **Leverage an access risk classification system** to gain a contextual understanding of risk across information resources as well as users and their roles/entitlements. A continuously and readily available view of enterprise-wide entitlements enables managers to concentrate their attention on the most risk-laden applications and levels of access to those applications. For example, a user's access to the organization's intranet may represent a relatively low level of risk, while an entitlement to access an application containing sensitive customer, employee, or product information may carry a substantial risk to the organization. Ready visibility of these entitlements makes it relatively easy to focus on the truly critical points of vulnerability. Such a system at Société Générale would have identified separation-of-duties violations in the rogue trader's array of access entitlements and alerted the appropriate managers.
3. **Instantiate policies through an automated governance platform** that enforces them in a consistent manner across the entire enterprise. Dynamic risk monitoring at Société Générale with key risk indicators to spot out-of-role entitlements, segregation-of duties violations and other compliance violations would have initiated an access certification review as soon as the rogue trader's inappropriate access was identified.
4. **Conduct a regular review of user entitlements** in which they are examined by business managers within the context of each individual's role. Verifying user identity is not enough; roles must be managed throughout their lifecycles in order to prevent high-risk situations resulting from entitlement drag. Société Générale managers should have been required to conduct periodic access reviews and recertifications in order to eliminate any existing segregation-of-duties violations or other inappropriate access entitlements.
5. **Automate the access rights remediation process.** Automation is the only way to ensure that the right people are quickly informed of policy violations, and that these are quickly dealt with, enabling corporate IT and security managers to effectively balance the demands of regulatory compliance and management of access-related risk, while effectively supporting the strategic initiatives of the business. By automating this

⁴ 2006 Annual Study: Cost of a Data Breach, Ponemon Institute

workflow, Société Générale would have been assured of a rapid resolution of all access-related policy and compliance violations.

With such a system in place, a large enterprise will be well on its way to managing the business and regulatory risks of inappropriate access to its applications and information. The right solution requires a strategic approach to access governance based on auditable business processes that enable line-of-business managers and information security, audit, and compliance teams to collaborate while ensuring accountability, transparency, and visibility.