

MANAGEMENT & STAFFING

Info-Tech Advisor Premium - Manage



About this research note:

Management & Staffing notes offer guidance on effectively managing people within an IT operation and dealing with associated leadership, staffing, and project management issues.

How to Lock Down Data Privacy at the IT Worker Level

Publish Date: January 23, 2006

Since IT staff has greater access to data than non-IT workers, the impact and risk of data theft committed by IT employees tends to be higher. Data integrity and security must begin with solid data privacy principles and practices. Align the enterprise's access controls with a privacy mindset to mitigate threats of data loss.

INFO~TECH
research group

Passionate About Research.
Driven By Results.



Executive Summary

Since IT staff has greater access to data than non-IT workers, the impact and risk of data theft committed by IT employees tends to be higher. Data integrity and security must begin with solid data privacy principles and practices designed to improve internal processes and protect the enterprise's critical information assets.

Some of the recommendations in this research note are better suited for larger enterprises that have the resources to put more stringent controls into place. However, smaller enterprises can also benefit from the compensating controls laid out in this research note. Topics discussed include:

- » How disgruntled IT staff can cause more damage to the enterprise's data assets than regular line workers.
- » The legislative requirements of data privacy and related laws.
- » A three-pronged plan of attack for delineating access control, including segregation of duties, least privilege, and identity management software.

Even though perimeter defenses are critical for preventing external attacks, internal threats must be acknowledged and addressed. Align the enterprise's employee access controls with a privacy mindset to mitigate threats of data loss or theft.



Management Point

Much attention is paid to data security and availability. However, many enterprises are legislated to maintain data privacy. Ensuring privacy means preventing unauthorized IT staff from accessing, modifying, copying, or deleting sensitive information such as credit card numbers, trade secrets, and other critical information assets. Acts of data theft and sabotage perpetrated by insiders is experienced throughout all industries and company sizes, but is one that is not widely reported by affected enterprises unless compelled by law to do so.

Stolen data can cost the enterprise in terms of lost business, loss of shareholder confidence, legal fees, and computer forensic fees. For example, a case of data theft committed by an employee cost two recruiting firms an estimated \$3 million between them. There is also the risk of hefty fines if the data theft is a violation of legislative requirements.

IT staff usually has greater access to data, and is thus able to cause more damage if so inclined. Consider this fictitious scenario:

1. Bob is a junior Database Administrator (DBA) responsible for maintaining a financial database. This database is used to disburse checks to customers. Bob requires read-only access to do his job and should not have the ability to actually change customer records.
2. One day, Bob decides that he would like to change a customer record to his own name and address, thereby allowing him to issue checks to himself. Bob then gains access to the database, directly altering the information in a customer record and bypassing controls present at the application layer.
3. Because Bob is accessing the file at the database level, rather than the application level, no audit trail of his action exists. Management is required to sign off on all checks, but because management signs hundreds of checks per day, Bob's fraudulent actions are not intercepted.

The requirement for management signoff is a perfect example of an ineffective manual control. An auditor would immediately label Bob's ability to alter customer data – as well as the IT system's inability to document, log, and audit this occurrence – a material weakness and produce a negative audit result for the enterprise.

In a privacy-focused IT environment, Bob would be blocked from the database in the first place due to rigorous access controls based on segregation of duties or least privilege. Even if Bob does try to access the database, his access rights are configured according to duty segregation policy. The system will therefore log the occurrence automatically, generate an alert, and notify management immediately.

From there, the appropriate actions can be taken against Bob, as per corporate security incident handling policies. This demonstrates how a change in process can transform a weak data privacy control into a preventive and automated mode that is highly effective.



Key Considerations

Addressing the issue of data privacy requires a three-pronged attack:

1. Segregation of duties.
2. Least privilege.
3. Identity management software.

Such an approach helps ensure that duties and areas of responsibility are separated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets, while the ID management tools enforce policy at the technology level.

Data privacy is called for in governance frameworks such as COBIT and ISO 17799, but is also a requirement of several privacy and fraud-related laws:

- » Sarbanes-Oxley (publicly traded companies)
- » FISMA (federal government and government contractors)
- » Basel II (international banks)
- » PCI DSS (merchants and credit card service providers)
- » GLBA (banks and financial services institutions)
- » HIPAA (healthcare providers and payment plans)

Segregation of duties is conducted for the purposes of determining who has access to the enterprise's systems and processes, and where potential conflicts may exist. Conflicts arise when an employee's job responsibilities overlap into another area, possibly allowing financial fraud to occur. Ensuring proper segregation of duties minimizes these conflicts, enhances data privacy, and creates compliance with Section 404 of Sarbanes-Oxley.

- » Segregation of duties is considered a type of internal control. Failure to adequately demonstrate the effectiveness of internal controls could lead to a negative audit outcome. In the case of non-traded companies (i.e. those that aren't governed by SarbOx), duty segregation should be viewed as a best practice that will improve security and help eliminate conditions wherein employee fraud could transpire.
- » But segregation of duties can also be used for IT departments at an operational level to improve error rates and increase reliability. For example, an application development team may have its duties segregated so that code writing, testing, and deployment are each conducted separately by three individuals, thus helping to ensure code integrity.



Least privilege, on the other hand, is not a requirement but is considered a security best practice. Least privilege is a principle of security in which IT staff is granted the absolute minimal level of access rights required to complete their duties. Least privilege requires the mapping of access rights to business requirements.

- » Intermittent elevation of access rights for IT workers will sometimes be required for a certain project. Still other IT staff will require full access to their machines' capabilities. Applying least-privilege principles to access policies in general will allow IT to customize security mechanisms according to business needs.
- » On the vendor side, Microsoft is currently promoting its Least-Privileged User Account (LUA) concept, which will be supported by the upcoming Vista operating system. The LUA construct acknowledges that new user accounts are set to "Administrator" as the default setting in Windows installations. LUA removes this danger by resetting user accounts to limited access configurations.

Identity (ID) management is a technology component that will be needed to help enforce, automate, and log user activities as they relate to data access and privacy. Identity management is a broad term meaning a system or solution that identifies individuals within the network, and then controls their access to network resources by associating user rights and restrictions with the established identity.

- » ID management software typically encompasses a combination of password synchronization/reset/recovery, single sign-on, digital certificates, tokens, and policy-based access management software.
- » The main value of ID management is that it eliminates manual user provisioning and access rights processes. In order to achieve this value, focus efforts on automatic process facilitation based on business, IT, and user needs.
- » ID management also brings new efficiencies such as fewer calls to the help desk, shorter call resolution time lapses, faster authorization and signoff, and so on.

Recommendations

1. **Create and/or amend policies and job descriptions.** Policy must drive and direct worker roles, responsibilities, and obligations as they relate to data privacy. Download and customized the following relevant templates from Info-Tech Advisor:
 - » Non-disclosure and non-competition forms (to protect sensitive data, corporate assets, trade secrets, etc.).
 - » Systems administrator code of conduct (for establishing a professional code of ethics for IT staff using sensitive data).



- » [Account privileges and expiry policy](#) (for closing old network IDs, e-mail accounts, etc.).
 - » Job description templates such as [Chief Privacy Officer](#), [Corporate Compliance Officer](#), [IT Controls Auditor](#), and [Security Analyst](#) (to define roles and responsibilities for creating and preserving data privacy).
 - » [Employee manual](#) (encompassing technology acceptable use policies).
2. **Apply the principle of least privilege, with caution.** Issues with the least privilege approach are twofold. First, least privilege requires the enterprise to plan and test limited access configurations, which can raise costs significantly. Costs may include help desk support, custom programming, additional tools, and changes to policies or procedures. Secondly, some applications will not work properly unless they are operating in administrator mode. This can create productivity issues for power users accustomed to browsing and downloading at will. Furthermore:
- » **Least privilege must be a component of an effective security model.** Some users simply should not have access rights to disable desktop firewalls, delete registry keys, and so on. Security strategy is about taking control and responsibility away from the users and giving them back to the business. From a technology perspective, least privilege means that if users are restricted completely from certain access rights, then those users do not require protection in the form of some type of security software.
 - » **Least privilege involves a shift in focus.** Least privilege requires IT management to adopt a mindset that embraces holistic security. For example, acceptable use policies would have to be rewritten to incorporate least privilege values. In-house developers would also have to integrate least privilege into their work.
 - » **User accounts must be appropriately organized.** One way to tackle least privilege is to log and monitor data transfer activity throughout the enterprise, and then restrict employees to transferring data from designated folders only. This process can be administered by combining patch management and policy enforcement software.
 - » **Deploying least privilege may cost money, but enforcement is free.** File transfers and application usage are traceable using audit trails. Configure the network to look for such activity and log these transactions for auditing purposes. To do this, IT administrators are using free security tools such as [Regmon](#) and [FileMon](#) from [Sysinternals](#). Regmon monitors applications accessing the Windows Registry, while FileMon monitors and displays file system activity. IT can also deploy a group policy across all domains to prevent all non-administrator accounts from downloading software.



3. **Update access rights on a regular basis.** Close monitoring of access rights is critical in any enterprise, but is also crucial for proper segregation of duties. Regular auditing and updating of user accounts will ensure that all accounts belong to legitimate account holders and that no former account holders have access rights once they have left the enterprise. Audit all access rights for:
 - » Company-based desktop and laptop PCs with approved software suites.
 - » IP accounts for e-mail and Web browsing, including intranet.
 - » Access to shared production server and main shared applications server.
 - » VPN access to the above services.
4. **SMEs must deploy compensating controls.** ISACA concedes that multiple job roles may be filled by a single person in a small IT shop. Situations such as these should be covered by compensating controls. Compensating controls are used to mitigate risk when appropriate segregation of duties cannot occur due to an SME's limited resources or smaller IT department size. If this is the case, deploy compensating controls that are considered sufficient and acceptable, such as:
 - » Audit trails of data transactions (i.e. who initiated them, when, why, and how).
 - » Reconciliation of financial applications.
 - » Exception reporting and handling oversight at the managerial level.
 - » Unalterable transaction logs or a journal of all transactions processed.
 - » Supervisory reviews of procedures to detect errors and irregularities.
 - » Independent reviews of procedures to detect errors and irregularities.
5. **Create a job duty matrix.** For reference on what an IT job matrix should look like, see Exhibit 2.2 in "[Segregation Of Duties Within Information Systems](#)" from the Information Systems Audit and Control Association ([ISACA](#)). This document will explain how to segregate duties amongst IT staff. Bear in mind that matrices will differ from company to company, depending on the size of the IT department and the enterprise's level of IT complexity.
 - » Duty segregation involves isolating, separating, or shifting critical responsibilities or access to systems. Critical responsibilities are defined as any combination of duties that could be used in concert to misappropriate data in such a way that the fraud would go undetected within a certain timeframe.



- » The matrix below, see Table 1, is a partial derivation from the CISA Review Manual 2006, an important reference guide for auditors developed by the ISACA. The ISACA concedes that the matrix is to be used as a rough guideline and not an industry standard. As is often the case, judgments about control effectiveness are left solely to the professional discretion of the auditor.

Table 1. Sample Segregation of Duties Matrix

	Control Group	Systems Analyst	Application Programmer	Helpdesk Manager	End User	Data Entry
Control Group		X	X	X		X
Systems Analyst	X			X	X	
Application Programmer	X			X	X	X
Helpdesk Manager	X	X	X		X	X
End User		X	X	X		
Data Entry	X		X	X		

X = Combining these roles may create a privacy conflict and control weakness.

6. **Invest in ID management tools.** ID management provides a high level of control redundancy by allowing IT to mitigate data breaches and reduce or eliminate material damage that can result from those breaches. Since compliance is the main watchword for many enterprises, an ID management initiative should have the capability to be audited internally. This will help bring close scrutiny to holes in risk management, as well as hasten regulatory compliance via thorough documentation of security controls.



- » An ID management solution can cost anywhere from between \$20 and \$50 per user, often for a minimum of 1,000 users per year. Implementation can take from six to twelve months to complete, depending on the size of the company.
 - » ID management vendors include [Computer Associates](#), [Courion](#), [HP](#), [IBM](#), [Novell](#), and [RSA Security](#).
7. **Microsoft Active Directory shops should use available tools.** Active Directory is a proven method for deploying access rights and role-based access control across the enterprise. In addition, the [Group Policy Management Console](#) add-on for Windows Server 2003 performs such tasks as file deployment, application deployment, logon/logoff scripts and startup/shutdown scripts, domain security, IPsec, and so on. Group Policy is available for free to Windows Server shops, and is also being integrated into Microsoft's Desktop Optimization Pack for Software Assurance.

Bottom Line

Data privacy is a pressing and growing concern for all enterprises. Segregate duties and tasks at the operational level to create an IT environment based on security best practices like least privilege.

FREE IT Benchmarking!

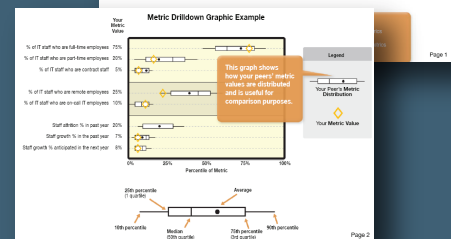
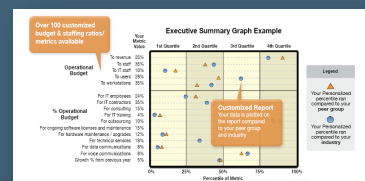
Under budget pressure? Need to justify every dollar you spend? Info-Tech's new program is designed to provide real world answers to your IT budget and staffing questions.

Start my custom survey

Begin your metrics program now with our survey and you'll receive:

- 8 Info-Tech Research reports on reducing your IT costs, rich with over **50 cost reduction strategies, 100 recommendations & 200 pieces of related research, tools & case studies**
- 2 detailed benchmark reports on budget and staffing, customized for your company
- Metrics compared to peer companies of similar size in your industry

There is no cost to participate, no sales person will call you and the survey takes only 15 minutes to complete.



Sample Benchmark Reports