Centrify®

TOP 3

Reasons to Give Insiders a Unified Identity

Although much publicity around computer security points to hackers and other outside attacks, insider threats can be particularly insidious and dangerous, whether caused by malice or employee negligence. In its list of the eight most significant cybersecurity threats for 2013,Forbes cited internal threats as No. 3, noting that internal attacks can be "the most devastating" due to the amount of damage privileged users can inflict and the type of data they can access![1]

One factor that exacerbates insider threats is that they can easily slip under the radar and avoid detection for a long period of time. According to the Forbes study, which was funded in part by the U.S. Department of Homeland Security and the U.S. Secret Service, malicious insiders in the financial industry were typically able to get away with fraud for nearly 32 months before being detected.[2] And it's not just malicious insiders creating such risks. Organisations also need to be concerned about a growing attack surface within their environments and problems resulting from users having too much privilege.

It is of great importance that high-level executives and IT compliance officers recognise and acknowledge the danger of malicious insiders, an increased attack surface and the potential for breaches caused by employee error or negligence. It is similarly vital that organisations support the deployment of technology solutions that can address such threats across the enterprise and enable mitigation as quickly as possible. Any delays in taking action will expose the organisation to additional risks and make it that much more challenging and costly to install effective solutions.

[1] "The Biggest Cybersecurity Threats of 2013," Forbes, Dec. 5, 2012

[2] Ibid

TOP 3 Cont.

Why the emphasis on insider threats, and why now? Several reasons:

1. Insider security risks are more prevalent and potentially more damaging: According to a study conducted by the Ponemon Institute, 34% of data breaches in the U.K., come from malicious activity, including criminal insiders, and 37% of breaches come from employee negligence.[3] A previous Ponemon study indicated that a third of malicious attacks come from criminal insiders.[4] Further, a Forrester study revealed that 75% of data breaches were caused by insiders, most often due to employee negligence or failure to follow policies. The most-often cited incidents were lost devices, inadvertent misuse of sensitive information and intentional theft of data by employees.[5] The impact of data breaches and downtime, whether caused by insider malice or negligence, can cripple an organisation, exposing it to lost revenue, significant brand damage and increasingly onerous regulatory fines and penalties. The costs to U.K. organisations suffering data breaches averaged more than £2 million per incident in 2012.[6]

2. User identity "blind spots" are causing audit failures: Many organisations are failing audits because of blind spots in their identity infrastructures. Blind spots can occur when identities and entitlements are managed in disparate silos or on local servers rather than centrally. For example, one of the biggest identity challenges for companies — and a major cause of failed audits — is a lack of visibility into local administrator accounts on Windows. This is akin to the root account on a Linux/Unix system. Failed audits can be particularly damaging in today's environment, in which regulations related to data loss and data protection are becoming more rigorous around the world. Companies that conduct business globally have to be in compliance with a wide range of rules and regulations to satisfy audit requirements.

As such, organisations must be able to provide proof that users who have access to certain servers and applications are actually authorised users. They must also be able to deliver an auditable trail of what each user has done within the server. These requirements mean organisational policies need to apply the principle of "least privilege access," whereby users log in as themselves and have only those privileges needed to do their jobs. If they need to have their privilege elevated for some reason, that is an explicit action.

[3] 2013 Cost of a Data Breach Survey, Ponemon Institute and Symantec, June 2013

[4] 2010 Cost of a Data Breach Survey, Ponemon Institute and Symantec, March 2011

[5] "Most data breachescome from within," Info Security, Sept. 24, 2012

[6] Ibid , footnote No. 2

TOP 3 Cont.

3. Organisational complexity is posing a growing challenge: Managing employee identity used to be relatively easy: A user was typically sitting at a desktop with a single machine connected to an enterprise application through a single wire. Ah, but things have changed. Users are now mobile and using a wide range of devices, some of which may be unsanctioned or undocumented personal devices. And mobility is only one aspect of the heightened complexity. IT infrastructures are increasingly diverse and heterogeneous, with multiple silos defined by departments, applications, operating systems or other characteristics that set them apart from one another. The proliferation of virtualisation and cloud services adds additional layers of complexity to the IT environment. Without a solution to unify user identities, organisations face the prospect of having too many identities, thus raising too many identity-related risks — including data loss, data breaches, application downtime, failed audits and an inability to identify and rectify internal security problems before they escalate.

Savvy IT and security managers are recognising that the most cost-efficient and effective way to address these challenges is to incorporate a solution that provides insiders with a unified identity across all platforms. By linking access privileges and activities to specific individuals, the IT organisation can establish the control needed to minimise security risks, along with the visibility required to achieve compliance.

Ideally, the unified security solution should be able to support heterogeneous environments, unify all identity policy — for authentication, authorisation and audit — and enable centralised identity management through a "single pane of glass."

Organisations can also achieve significant benefits in terms of costs savings and deployment speed by leveraging a unified identity solution on top of an existing platform, particularly Microsoft Active Directory. Because of its ubiquity and ability to handle some of the underlying functionality of unified identity management, Active Directory offers many advantages:

Why give insiders a unified identity? And which solutions give you the best opportunity to reduce costs and reduce risks? Here are the top three reasons to give insiders a unified identity.

#1 Reduce the risk of audit failures, insider threats and other security breaches.

Before we delineate how use of a unified identity reduces risks for the organisation, let us describe what is meant by a unified identity and how that identity should be managed across the enterprise.

With a unified identity, an insider has a single login across Windows, Linux and Unix servers. Insiders can access only those systems and applications necessary to perform their jobs, and all of their administrative activities must be tied back to their identity.

Unified identity also means that authentication, authorisation and audit policies are unified as well. The IT organisation should have full visibility into all of the systems each user has access to, as well as the elevated privileges each user has within each system. The IT department should also be able to fully audit what each user does with those privileges, down to the commands they execute and full session capture.

The ability to create a unified identity for each user within the organization and centrally manage, monitor and audit the activities of each user significantly reduces the risks of audit failures, insider threats and other security breaches by:

- Establishing visibility into your risk posture.
- Identifying blind spots in your server environment, such as the lack of visibility into local administrator accounts on Windows.
- Ensuring consistent policy management and enforcement for authentication, authorisation and auditing across the entire enterprise.
- Providing auditors with proof of who has access to what — and what they have actually done with that access.

TOP 3 Cont.

#2 Lower TCO through a simplified and standardised approach to managing identity-related risks.

IT environments are increasingly heterogeneous, which means they can be increasingly complex. You can't rip out and replace your entire infrastructure, but you can address the identity management challenges of heterogeneous environments with a unified identity management solution that offers these key features and functions:

- Support for all platforms in use across the enterprise. This is critical because, as noted, most organisations are highly heterogeneous and the same user is often logging into multiple systems. As an example, you want to be able to manage identities for Windows, Mac, Unix and Linux platforms all from the same place, with consistent policies and unified user identity.
- Ability to centrally manage the entire ID policy through a single pane of glass for policy management, monitoring, auditing, and compliance reporting.
- Ability to leverage investments in existing identity infrastructure by deploying Active Directory. Managing the identity infrastructure from a central place using Active Directory as the foundation delivers a wide range of benefits that will lower total cost of ownership, specifically:
    - No need to rip out and replace your existing identity management infrastructure.
    - No need for IT to invest time, energy and money in training to learn a new system.
    - No need to invest in a brand new platform.
    - No critical business time lost due to a transition to a new platform.
    - Accelerated time to value by leveraging existing investments in the identity infrastructure.

In terms of overall costs, it is important that IT and security professionals consider the potential costs of a failed audit and/or a data breach. The fact is that many organisations are failing audits due to challenges related to the complexity of their existing identity management infrastructures, along with concurrent gaps in their operational procedures.

Audit failures occur when the organisation has inconsistent password policies — or no policies — and is unable to document and prove who accessed certain applications, what types of authorisation rights they had and what they actually did (or did not do) when they performed a specific operation.

With the right solution in place, the organisation can simplify the management of insider identities and seamlessly prove compliance — putting in place password policies, proof of policies for privileged users and visibility into access controls. The key is that visibility, monitoring and enforcement all stem from a centralised management function that is controlled by IT.

Historically, the challenge has been to manage diverse platforms together with consistent access policies and, with respect to the data center, to manage them using the existing infrastructure. Managing user identity through one pane of glass can resolve that challenge, enabling integrated control of user access and auditing across all platforms — Windows, Unix, Linux and others — on-premises or in the cloud.

#3 Securely support next-generation IT and business initiatives.

Enterprises need solutions that support the deployment of the critical initiatives that are driving next-generation applications. IDC has characterised the combination of cloud services, social networking, mobility and big data as the next major compute platform, driving 80% of spending growth between now and the end of the decade.[7]

TOP 3 Cont.

However, each of these initiatives brings the potential of new insider threats to the organisation. As noted by Gartner:

The opening up of enterprise systems information assets and business processes brought about by social networking, exposure to the cloud, mobile devices (especially consumer-owned devices and big data) brings with it a whole new set of security and privacy concerns... As hacktivists, organised crime and nation states increase the pressure, enterprise security must evolve, particularly to counter the increasing risk from insider threats and targeted attacks.[8]

In this environment, organisations must be able to empower their employees to take advantage of these initiatives, but they must do so in a way that protects the enterprise from potential damage and risk, and with far less concern about failing audits or losing revenues/opportunities due to problems caused by insider threats.

This requires an identity infrastructure that is simple to scale, simple to manage and increasingly dynamic, enabling secure support for new business initiatives on an enterprisewide scale. By leveraging the existing investment and focusing on a unified identity policy, organisations will be able to support inside users while also:

- Leveraging a sound investment in unified identity management.
- Continuing to leverage secure identity management as a strategic asset moving forward.
- Protecting the investment and eliminating the risk of dead ends while embracing next-generation initiatives.

Moving forward

The business case for giving insiders a unified identity is clear and compelling: lower TCO, reduced risk of data breaches, reduced risk of failed audits, a more agile identity infrastructure, improved time to value and support for next-generation business initiatives. One of the first steps in moving forward is to work with a vendor partner that truly understands the challenges — and opportunities — in unified identity management.

Centrify is a clear leader in unified identity management, offering a complete integrated solution for identity consolidation, authentication, single sign-on, group policy enforcement, privilege management and auditing across the broadest set of platforms in the industry, on-premises and in the cloud. Centrify integrates heterogeneous systems and applications into a secure, connected computing environment with Active Directory at the center.

The Centrify Server Suite simplifies the management, enforcement and visibility of identity-related risks — anticipated and unanticipated — by providing a unified identity infrastructure with a single identity for users and a single identity infrastructure for IT. The Centrify suite provides coverage of more than 400 different platforms and is nonintrusive to the existing Active Directory infrastructure, requiring no schema modifications and no software installed on domain controllers.

If your organisation has missed a security audit or hasn't taken the proper steps to address the growing challenge of insider threats, it is certainly time to get started, before risks turn into reality. Are you ready to learn more? Contact Centrify.

About Centrify

Centrify provides Unified Identity Services across the data center, cloud and mobile that results in one single login for users and one unified identity infrastructure for IT. Centrify's solutions reduce costs and increase agility and security by leveraging an organization's existing identity infrastructure to enable centralized authentication, access control, privilege management, policy enforcement and compliance. Centrify customers typically reduce their costs associated with identity lifecycle management and compliance by more than 50 percent. With more than 5,000 customers worldwide, including 40 percent of the Fortune 50 and more than 60 Federal agencies, Centrify is deployed on more than one million server, application and mobile device resources on-premise and in the cloud.
For more information about Centrify and its solutions visit http://www.centrify.com/.

[7] "IDC Predicts 2012 Will Be the Year of Mobile and Cloud Platform Wars as IT Vendors Vie for Leadership While the Industry Redefines," IDC, Dec. 1,2011

[8] "The Nexus of Forces Changes Everything," Gartner Symposium/ITxpo 2012 Keynote, Jan.10,2013