

Compliance pitfalls with high-risk users

Date: December 1st, 2008

Author: Cheryl Traverse

Category: General

Tags: Compliance, Cheryl Traverse, Security

A secret most security vendors will not tell you is high-risk users may circumvent traditional network and security compliance controls every day. Because of this, it is important to examine best practices, and take needed action to control high-risk users.

As CEO of a company that works extensively to understand and control the threat of high-risk users, I have found that there are practical and cost-effective steps that should be executed to build on existing access policies and controls.

To begin your company's action plan to control high-risk users, I wanted to answer some of the important questions I'm asked by clients. The answers to these questions will:

Provide a definition of the high-risk user.

Explain why common security practices do not go far enough.

Outline six questions that you must answer to help select the right entitlement management solution.

Define how entitlement management is an important part of the solution.

Describe how entitlement management helps organizations force high-risk users into a trusted and compliant state.

High-risk users and compliance pitfalls

With today's information security compliance mandates, boards of directors and executive management are being held accountable for protecting sensitive corporate information and preventing material events, such as a data breach, that could negatively affect shareholder value. Understandably, organizations are allocating major resources to ensure they have adequate security controls in place, especially concerning trusted insiders.

Unfortunately, most security vendors and organizations focus security compliance controls on the ordinary user risks - ignoring the high-risk user. High-risk users have the technical knowledge and tools to create major havoc. They create a paramount challenge to the stability of infrastructure security. On the one hand, privileged access for high-risk users is a necessary aspect of daily operations. On the other hand, it's a black hole that prevents companies from

enabling security compliance with regulations including Sarbanes-Oxley, PCI and HIPAA.

According to a study by CERT at the Carnegie Mellon University's Software Engineering Institute, a recent profile of insider attacks showed that a company is most vulnerable from high-risk users - internal and external. Eighty-six percent of insider attacks were either previously or currently employed full-time employees in a technical position within the organization.

Now, more than ever there is an urgent need for companies to adopt entitlement management strategies for high-risk users.

Balancing high-risk users and operational efficiency

Entitlement management allows an organization to control user access to the critical infrastructure, enforce granular access policy, monitor activities, record events, and view centralized compliance and testing reports to validate that controls over high-risk users are working. A cost-effective entitlement management solution should establish a security compliance approach that reduces the complexity and cost of managing the risk by addressing the specific circumstances. Common security strategies focus on the risk of data loss from the ordinary trusted user. The pitfall to this security strategy is that there is a harsher threat - the high-risk user.

Six questions about the high-risk users in your organization

All companies should be asking themselves six questions:

- Do we have high-risk users with daily access to our critical IT infrastructure?
- Do we have a way to manage these users to a limited access as they work inside our infrastructure?
- How do we grant access to remote and local high-risk users to guarantee that they only access the approved systems?
- How do we monitor every aspect of what high-risk users are doing in our applications and networks?
- Can we record high-risk user activity to create an irrefutable audit and forensic trail that proves to auditors that we have adequate, working controls in place?
- Can we easily produce comprehensive compliance and testing reports?

As you address these six questions, you'll begin to establish a foundation of knowledge that will help you define the framework of your entitlement management strategy.

Improving security and demonstrating compliance

Entitlement management technology has proven useful by providing firms with a variety of new tools to boost security with practical solutions. Some things to consider in selecting these types of solutions include evaluating their ability to:

Control access with enforceable access policies and user IDs to contain high-risk users.

Integrate high-risk user policies with existing security systems.

Centralize a company's view of high-risk user activities.

Compartmentalize high-risk users to specific applications and areas on individual network devices and virtual environments.

Monitor, track, and record command line sessions, key-strokes, and screen images to create a full and detailed audit that proves these controls are in place and work effectively.

Establish compliance reporting and testing to validate that the controls are working.

With controls in place the level of efficiency with which the firm can run is much higher, not to mention an elevated degree of internal trust that improves a company's routine operations.

Unfortunately most companies' security practices are noncompliant for high-risk users.

Companies must identify prudent steps and best practices to implement cost-effective entitlement management solution for compliance. The right entitlement management strategy that leverages the proper technology controls forces high-risk users into compliance with legal, regulatory, and corporate security mandates.

About the Author:

Cheryl Traverse is CEO at Xceedium. She previously served as CEO at Immunix. Prior to this, Cheryl served as CEO for Covigo Inc., Taviz Technology and brightinfo.com, and as an EVP at iBand. She also held executive management positions at Sprint, MCI and Gupta Corporation. Cheryl holds a BA degree from Wilkes University and an MS degree from Hofstra University.

Get weekly leadership tips in your inbox

TechRepublic's IT Leadership newsletter, delivered each Tuesday and Thursday, offers tips for how to effectively manage your staff and your IT infrastructure. Automatically sign up today!

People who read this, also read...

What you can learn from outstanding leaders

How to work with a headhunter

Shifting from compliance to security requires patience

Take the guesswork out of your business decisions

The business case: What to do after the pitch

Trackbacks

The URI to TrackBack this entry is: *http://blogs.techrepublic.com.com/tech-manager/wp-trackback.php?p=646*

No trackbacks yet.

[My Updates](#)

[My Contacts](#)

Would you like your own dynamic Workspace on TechRepublic?

Take two minutes and set up a TechRepublic member profile.

[Sign In Now](#)

Would you like your own dynamic Workspace on TechRepublic?

Take two minutes and set up a TechRepublic member profile.

[Sign In Now](#)

Popular on CBS sites: [CES](#) | [Spore](#) | [iPhone 3G](#) | [Katy Perry](#) | [Antivirus Software](#) | [GPS](#) | [Recipes](#) | [Macworld](#) | [NFL](#)

[About CBS Interactive](#) | [Jobs](#) | [Advertise](#) | [Mobile](#) | [Site Map](#)

© 2009 CBS Interactive Inc. All rights reserved. | [Privacy Policy](#) | [Terms of Use](#)