

Search: (Advanced)

CW Print Ref.
Code

COMPLIANCE WEEK

Doug Juenemann

- Your Account
- Sign Out

June 26, 2007

Subscriber Assistance

888-519-9200 Or Email Us

Contacts, Masthead

Sections & Coverage

Archives

Columnists

Harvey L. Pitt

Richard M. Steinberg

More, Plus Guest

Columns

GRC Illustrated

Guidance & Commentary

Q&A Interviews

Remediation Center

Rules & Standards

Topic Index (ERM, ICFR)

Disclosures & Databases

Weekly Auditor Changes

CD&A Disclosures **NEW**

10,000+ Corporate

Charters

Internal Control

Disclosures

Investigations & Probes

MD&A Risk Factors

More Disclosures

Other Features

Compliance Solutions,

Firms

Help Wanted; GRC Jobs

Printable Home Page

Knowledge Leadership

Compliance Week Live

2007 Annual Conference

Live Webcasts

More Conferences, Events

 PRINTABLE VERSION

Effective Access Control: Communication, Simplicity

By Todd Neff — May 22, 2007

The need for a fancy identity-management system to control access to IT systems depends on how big and complex you are and how much pain your company can take. Linda DiPaola, with less than 500 employees to track, does just fine without any system at all.

DiPaola, director of internal audit at Empire Resorts, a New York gaming and resort management firm, depends on process, not technology, and it's working perfectly well.

DiPaola says her approach is all about managing risk. From an access control perspective, that means upholding the sanctity of segregation of duties and ensuring that user permissions to IT systems match business needs. There's also making sure departures, promotions, and the like prompt changes to user access appropriately.

Empire Resorts consists of a host of many nonintegrated systems, DiPaola explains, so she watches just two systems closely: the financial reporting and gaming applications. If she were to monitor much more, "we'd have to hire another person," she says.

Once a week, Empire's personnel department notifies the IT department of new hires, transfers, and departures. Once a year, the IT staff prints out its access list and sends it to department heads, who confirm or question the access of users they should know personally. The system works, DiPaola says.



Gilbert


But size does matter, according to Jackie Gilbert, a cofounder of identity management software maker SailPoint Technologies. The Sarbanes-Oxley Act does require reviews of user access, as part of its Section 404 provisions around internal controls over financial reporting. But a "scan the spreadsheet printout" approach is hardly practical for large organizations with thousands of employees.


Complicating matters is a cultural barrier between IT and business functions. SailPoint recently commissioned an independent survey by the Ponemon Institute, published in late February. Among the survey's most alarming findings: Two-thirds of the 627 respondent companies said their IT and business functions collaborated rarely or not at all on identity management.

"The tech guy doesn't know the people and business roles," Gilbert says. "The business manager knows the people, but doesn't understand the cryptic permissions."

Then there's the issue of review frequency. Most of the 100 companies SailPoint surveyed go through IT access reviews, Gilbert says. "A few do it annually. These appear to be the ones who are really good at

RELATED COVERAGE

 Privacy And Data Protection Risks (April 24, 2007)

 Taking A Holistic View Of Risk And Privacy (Jan. 17, 2007)

 Building Compliance Efforts With IT Roadmaps (June 20, 2006)

 Managing Privacy Compliance As A Public Company (May 31, 2006)

 MIT Researcher Talks IT Risk And Impact On Enterprise (Nov. 22, 2005)

Related Webcast

 Don Nicolaisen On The Future Of Access Controls (June 28, 2007)



Assistance

[About Compliance Week](#)
[Who Subscribes?](#)
[Testimonials](#)
[Contact Us](#)
[How To Subscribe](#)
[Writers Wanted!](#)
[Terms Of Use](#)

managing their auditors, and I'd argue it's less effective of a control."

For a major financial service firm with tens of thousands of employees and hundreds or thousands of applications to access, "doing that sort of quarterly access review is quite a nightmare," Gilbert says.

SailPoint is one of many software firms in the business of automating such processes. Others include major players such as Computer Associates, Microsoft, Oracle, IBM, Novell, Hewlett-Packard, Sun Microsystems, and EMC as well as dozens of smaller companies.

Like DiPaola, William Baumer has so far resisted taking the identity-management technology plunge. Baumer, senior vice president of compliance and audit for First Marblehead Corp., said in an e-mail that his company is considering single sign-on solutions to strengthen access controls and make life easier for the roughly 1,000 employees at the student loan bank. But, he says, "We are finding that the solutions are very expensive and difficult to justify from an ROI perspective."

Baumer is not alone in his sticker shock. The Ponemon survey found that half the responding organizations with fewer than 5,000 employees viewed the cost of such systems as a major obstacle. But the survey also indicated that 59 percent of respondents in companies with less than 5,000 employees used identity-management and access-management software anyway (a full 67 percent of those with more than 5,000 employees did).

In terms of access rights, Baumer says First Marblehead uses a "least privilege" model, where the employees receive the minimum access required to get their jobs done. New access requires permission from the worker's immediate manager, the data owner, and in extraordinary circumstances, the chief information security officer.

Creating ID Systems, And Using Them

Despite the apparent penetration of access-control systems, half the respondents said they were unable to manage identity, the Ponemon survey found.

This should come as no surprise. Access controls have had it rough since mainframes gave way to IT architectures involving distributed computer systems on every employee's desktop. By the time access-control software tamed the chaos of controlling user access to complex and distributed IT systems (as opposed to one big-iron machine), the Web came along and made it cheap to invite suppliers, service providers, partners, and customers into the system as well.

Then Sarbanes-Oxley, HIPAA, PCI, Gramm-Leach-Bliley, and state breach notification statutes conspired to elevate what were mainly issues of data security and efficiency into vivid legal concerns.

The idea of "federated" identity management software is the latest to come along to address the Web-enabled world. It involves creating procedural and technical frameworks where partners assuage one another's angst regarding employees' mutual system access. But while that concept sounds good, the basics are often ignored.

"I can't tell you how many Fortune 500 organizations we talked to where the CFO hadn't changed his password in 3 years," says Justin Morrow, a partner with Control Solutions,

ID MANAGEMENT

Five Tips For ID Management

1. Understand your business requirements for IT access, which includes developing a good model of who should have access to what.
2. Determine who actually has access to what systems and applications.
3. Understand your business's risk profile and, based on the location and amount of critical data and who has access to it, where excessive exposure to risk exists.
4. Apply controls as appropriate to the risk level you're willing to accept.
5. Consider controls on multiple dimensions. One control might involve a regular review of who has access to what; another might consider the timing, location and nature of access—for example, a proper user doing major downloads on a weekend could raise concerns.



Morrow

which helps companies develop and test internal controls in advance of compliance audits. Or, he says, system administrator types with god-like “super-user” access status leave their passwords on Post-It notes stuck to monitors for anyone to read.

Solid access processes remain paramount, Morrow says, because without them, you can't establish a system capable of easily proving effective IT access compliance. But the landscape is getting so complex that technology is becoming more of a mandatory element in that effort as well, he says.

“I always used to tell people that it wasn't about technology; it was about process,” Morrow says. “Now we're starting to see how burdensome it can be without the technology.”

Morrow says his experience has been that a minority of companies has implemented more elaborate identity management systems, which can range from the low hundreds of thousands of dollars to about \$1 million. That spending, he explains, often takes the realization that access-control compliance reviews are costing hundreds of hours of consultant time to justify action.

“I think most organizations have to feel some pain before they will invest,” Morrow says.

Compliance Week provides general information only and does not constitute legal or financial guidance or advice.

© 2007 Financial Media Holdings Group, Inc. All Rights Reserved. "Compliance Week" is a registered mark of Financial Media Holdings Group, Inc.

Compliance Week provides general information only and does not constitute legal or financial guidance or advice.