Current Issue
Archive
Subscribe
Advertise

Web Exclusive Content
Home
HR News
HR News Analysis
Features
Columnists
Special Reports
Resources and Tools
Technology Center
Legal Clinic
HRE Conferences
HRE Rankings
RSS
Career Center
HR Internet Search powered by workindex
HRE Information
Subscription Center
Advertiser Information
About Us
Contact Us

Newsletter Sign-up
Click on the name of

Restricting IT Access

Workers have too much access to information at work, leaving companies vulnerable to compliance and risk issues, say IT executives. Human resource leaders need to ensure that appropriate policies are created -- and enforced -- and that organizations keep pace with changes in users' roles.

By Melissa Busch

Many IT executives believe employees have too much access to information that is not relevant to their jobs and that access policies are not regularly enforced.

That's according to the *2008 National Survey on Access Governance* recently released by the research firm Ponemon Institute, an independent research organization in Traverse City, Mich., dedicated to privacy-management practices, and the corporate security vendor Aveksa.

The study showed that more than three-quarters (78 percent) of the almost 700 experienced IT professionals surveyed believe information is too accessible and about seven in 10 (69 percent) felt that policies established to control access were ignored or poorly enforced.

Organizations are leaving themselves vulnerable to serious noncompliance and business risk by failing to govern access, says Brian Cleary, vice president of marketing for Aveksa in Waltham, Mass. He says the risks can materialize into legal fines and regulations, a loss of revenue and other significant costs.

"One disgruntled employee and a malicious act can be expensive," Cleary says. "If the action causes a business to lose millions of records, an organization could be looking at a $50 million expense."

Being too free with access also may cause damage to the company's brand, Cleary says.

"If an access issue causes a bank to lose your personal information, what's the first thing you're going to do," Cleary asked. "That's right, you're closing that account. The damage is done."

Gary T. Rich, of the executive advisory firm Rich Leadership in New York, believes the real concern is the "controls managed within a company."

"Having too much information, I don't see the downside," Rich says. "People need a lot of information to be effective. My problem is with the loss of control."

The study shows that organizations face several challenges, including user access being poorly assigned, policies not being checked or enforced, and organizations failing to keep pace with changes in users' roles, when implementing an effective access governance framework.

As "gatekeepers" of an organization, Rich says HR leaders must ensure that an access-rights system is in place that relates to indoctrination, termination and transition.

"This should include a regular review of what systems and applications employees have access to," Rich says. "Whenever there is a job change, that person's systems and access rights should be checked and re-approved and changed as necessary."

More than half (57 percent) of IT professionals reported that stakeholders do not collaborate to achieve access compliance within an organization, according to the study.

Inno Eroraha, chief security strategist and founder NetSecurity Corp. in Sterling, Va., agreed that detailed policies and procedures need to be established and enforced. He suggested quarterly reviews of the information available to employees and installing technology that tracks users' logons into systems.

But, Eroraha does not believe employees should have information that is not pertinent to their jobs.

"It should operate like the U.S. government -- on a need-to-know basis," Eroraha says. "If you don't need the information for your business [duties] then you shouldn't have them."

According to the study, three-quarters (74 percent) of those who participated in the survey believed that senior management does not view, or is unsure, access governance is a strategic security imperative.

This shows that "senior management still doesn't get it," Eroraha says. "All senior management cares about is the bottom line. They think, 'IT will deal with it.' But, senior managers have to be involved if they want to prevent problems."

Charles Caulkins, managing partner of law firm Fisher and Phillips in Ft. Lauderdale, Fla., says it is up to human resource professionals to help employees understand.

Caulkins says businesses must step up to the challenge of dealing with out-of-control access. Managers must be educated to recognize the importance of access governance and human resources executives must direct IT in matters related to this issue.

"Training and education of senior managers, especially those that handle sensitive material, need to be a part of this," Caulkins says.

February 19, 2008