

Activate your FREE membership today | Log-in

ADVERTISEMENT

case studies, downloads, and all the latest moves at easyeasier.com

Microsoft Forefront

SearchSecurity.com
The web's best security-specific information resource for enterprise IT professionals

HOME | NEWS | MAGAZINE | WEBCASTS | WHITE PAPERS | LEARNING | ADVICE | TOPICS | EVENTS | ABOUT US

SEARCH: [Advanced Search](#) | [Site Index](#)

Powered by:

ADVERTISEMENT **Microsoft** Case Studies, downloads and all the latest moves with Microsoft Forefront. [Click here to explore.](#)

[Home](#) > [Security News](#) > IT pros impede PCI, Sarbanes Oxley compliance

Security News:

[EMAIL THIS](#) [LICENSING & REPRINTS](#)

IT pros impede PCI, Sarbanes Oxley compliance

By Robert Westervelt, News Editor
08 Aug 2007 | [SearchSecurity.com](#)

RSS FEEDS: [Security Wire Daily News](#)
 [Add to Google](#)

Corporate IT professionals lack a critical understanding of risk and compliance issues and pose a barrier to collaborating on compliance initiatives with audit and compliance professionals, according to a study of 845 IT pros and audit and compliance managers conducted recently by the Ponemon Institute.

I think what they're saying is that IT practitioners care about their effectiveness and making IT better, but they don't care about compliance the same way compliance and audit people care.

Larry Ponemon,
founder and chairman,
Ponemon Institute

The study found that 65% of audit and compliance pros surveyed believe their IT counterparts lack the knowledge of risk and compliance issues to collaborate on identity and access management. In contrast, 42% of IT pros said audit and compliance managers lacked sufficient technical expertise to collaborate.

"I think what they're saying is that IT practitioners care about their effectiveness and making IT better, but they don't care about compliance the same way compliance and audit people care," said Larry Ponemon founder and chairman of the Traverse City, Mich.-based Ponemon Institute. "It's definitely true that collaboration is an issue and creating problems for identity or access management, but not clear if both sides share a common view of why those problems exist."

Experts say a number of high profile data breaches, such as the [massive breach earlier this year at TJX Cos. Inc.](#), is fueling spending on technologies that lock down data and monitor systems containing critical information. [But technology alone won't solve the problem of data leakage, experts warn.](#)

Collaboration between IT and compliance professionals as well as sound security policies are essential to keeping data locked down. Identity and access management is critical to compliance because it defines the process of an organization to allow end users to access systems containing critical data.

"A lot of people have the misconception that it's only technology, but it's also the control practices that an organization has in place," Ponemon said. "When people leave or move into new job functions, access rights change in conformance to what they are currently doing."

Compliance:

[Quiz: Must-have compliance technologies:](#) A five-question multiple-choice quiz to test your understanding of the content presented by expert Trent Henry in this lesson of SearchSecurity.com's Compliance School.

[PCI compliance costs often underestimated, study finds:](#) Companies are moving forward with PCI DSS projects, but many are underestimating

Ponemon said collaboration between IT and compliance and audit professionals is an important factor in reducing risk at an organization. IT pros also need to have the tools to assign access rights and change privileges when the organization changes. Compliance managers need to know whether access rights conform to the organization's policies and that the policy reduces the business risk, Ponemon said.

Meanwhile, an organization's business unit views identity and access control as a business need, he said. If end users can't access the systems they need to do their job, the business unit may step around IT and compliance managers by sharing a common password to bypass an access

REFERENCE DESK

Sarbanes-Oxley Act

NEWS, TIPS & MORE

- IT pros impede PCI, Sarbanes Oxley compliance (ARTICLE)
 - COSO and COBIT: The value of compliance frameworks ... (TIP)
 - Quiz: Ensuring compliance across the extended ... (QUIZ)
 - Is the Sarbanes-Oxley Act being enforced? (EXPERT ANSWER)
- [→ VIEW MORE](#)

VENDOR CONTENT

- Aligning Finance and Sales: Best Practices for Sales Compensation Management (WHITE PAPER)

ADVERTISEMENT

Microsoft

case studies, downloads, and all the latest moves at easyeasier.com

Microsoft Forefront

- Secure File Transfer in the Era of Compliance (WHITE PAPER)
 - Webcast: WS_FTP Server with SSH- The Smarter Way to Transfer Files (WEBCAST)
 - Evolution from FTP to Secure File Transfer (WHITE PAPER)
- [→ VIEW MORE](#)

SEE ALSO

- Related Topics:** Sarbanes-Oxley Act , Security Audit, Data Security Breach Laws and Notification, Data Privacy
- Site Highlights:** Quiz: Application Attacks
Quiz: Vulnerability Mgt.

GET E-MAIL UPDATES

Submit your e-mail below to receive Security-related news, tech tips and more, delivered to your inbox.

Compliance

Security Management

E-mail: Your E-mail Address

Not a member? We'll activate your FREE membership with your subscription.

the costs associated with compliance.

[COSO and COBIT: The value of compliance frameworks for SOX:](#)

In an attempt to blaze a path through the myriad of compliance regulations and requirements, organizations are looking to frameworks like COSO and COBIT.

[What are the PCI DSS compliance benefits of tokenization?:](#) Security expert Joel Dubin defines tokenization and discusses how the technology can help ease the burden of achieving PCI DSS compliance.

control system.

"I think IT people are coming to the realization that they have an important part to play in ensuring integrity and security of an organization," Ponemon said. "At the end of the day, IT has a lot of power but many times the business units have more control."

Both IT pros and compliance and risk managers agree that identity management and access control needs to be addressed to comply with current regulations and avoid a high profile data breach. According to the survey, 71% of compliance professionals believe identity and access management is "very important" or "important" for meeting compliance requirements within their organizations versus 70% of IT professionals.

But audit and compliance professionals may not feel comfortable collaborating with IT pros, Ponemon said. According to the survey, only 23% of respondents said they should be involved in the monitoring of compliance and 5% said they should be involved in shaping policy.

"The IT practitioners are more likely to own the creation of identity policy and fixing of deficiencies," Ponemon said. "It's hard to gauge the mindset of audit and compliance people in general, but there is a significant technology component that they may not feel comfortable with."

In addition, the study found that IT and compliance pros don't agree on what rules and regulations are driving compliance initiatives. Sarbanes Oxley and the Payment Card Industry Data Security Standards are ranked by compliance and audit professionals as the main drivers for spending on compliance projects in 2007. But IT professionals put much more weight into data breach laws and privacy laws such as the Gramm-Leach-Bliley Act and state data breach notification laws, than compliance professionals.

The Web survey was conducted independently by the Ponemon Institute and underwritten by identity and risk management vendor Sailpoint Technologies, based in Austin, Texas. Respondents averaged about eight years of experience in the audit or compliance field and more than three years of experience in the position they currently hold. About 50% of respondents said their job function or position is located within the corporate compliance department. About 22% said they report to the organization's chief financial officer, and 13% are located in the IT department.

Sound Off!  [Post your comments](#) | [See others' comments \(2\)](#)

Share - [Digg This!](#)  [Bookmark with Del.icio.us](#)

SECURITY RELATED LINKS

Ads by Google

[PCI Compliance](#)

Full IT Security Compliance for PCI DSS Section 10 & 11
www.eventlogmanager.com

[Sarbanes Oxley Audit](#)

Use our free checklist to evaluate corporate internal controls.
www.softrax.com/SOX-Checklist

[View our online Demo](#)

Does your Website measure up? Watchfire WebXM Can Help!
www.watchfire.com

[PCI/CISP/SDP + EV SSL](#)

PCI Compliance by AmbironTrustWave Audit, Scanning & EV SSL
www.atwcorp.com

[Security compliance](#)

Download IT White Papers About Security compliance
www.FindWhitePapers.com

RELATED CONTENT

• Sarbanes-Oxley Act

COSO and COBIT: The value of compliance frameworks for SOX
Quiz: Ensuring compliance across the extended enterprise
Log management push has its roots in compliance
Information security book excerpts and reviews
How should termination procedures address a user's multiple roles?
Is the Sarbanes-Oxley Act being enforced?
How to enforce a data destruction policy
Balancing Act
A new awareness for SIMs
SEC moves to ease Sarbanes-Oxley burden for some
Sarbanes-Oxley Act Research

• PCI Data Security Standard

Quiz: Must-have compliance technologies
Black Hat 2007: New database forensics tool could aid data breach cases
PCI compliance costs often underestimated, study finds
What are the PCI DSS compliance benefits of tokenization?