

# Identity Risk: *Are Insiders Threatening Your Compliance Efforts?*

By Mark McClain

Sabotage, espionage and financial fraud ... Attention-grabbing words that have been in the press all too frequently lately, ranging from the Prudential story about an IT staffer who was caught trying to sell the identities of 60,000 employees, to the recent DuPont incident, in which an employee compromised \$400 million in trade secrets. These are hardly confidence-inspiring times for corporate CEOs and their respective boards of directors.

Without a doubt, the past few years have been challenging ones for companies seeking to expand business operations in a climate of increased government regulation and heightened media attention and public scrutiny around security and privacy concerns. And while disruptive new technologies have created unprecedented opportunity for innovation, growth and productivity, they have also created unforeseen risks that companies are now being held legally and financially accountable for – to regulators, to shareholders and to the public at-large.

Much of this risk can be attributed to business initiatives that demand more open access to internal resources. Today, companies are providing employees, contractors, partners and suppliers increased access to sensitive enterprise systems and data – information that helps them drive revenue, improve customer relations or streamline operations, while at the same time opening them up to a potentially crippling security exposure. Unfortunately, determining where the greatest risks exist, and who is responsible for managing them, continues to be a largely ad hoc, reactive process – one frequently driven by a high-visibility incident involving thousands of innocent victims and potentially millions of dollars in damages.

Research results published in a recent Ponemon Institute *Survey on Identity Compliance* show that nearly 60 percent of IT security professionals in US-based businesses and government agencies believe they are unable to effectively assess or quantify “insider threat” risks within their organizations, leaving them open to privacy breaches, failed audits and potential fraud or misuse of data.

“Companies must focus their identity risk management efforts on the information assets that represent the most value – and potential liability – to the business.”

— Mark McClain,  
CEO & Founder,  
SailPoint Technologies

This is notwithstanding the fact that more than 80 percent of the 600-plus respondents surveyed agree that risk should be a determining factor in driving identity compliance initiatives.

So if everyone knows there’s a problem, why aren’t companies doing a better job of protecting their customers and ensuring the financial stability and corporate accountability of their businesses?

The Ponemon survey provides some interesting insights into the challenges that companies face. Although more than 70 percent of respondents confirm that identity compliance activities are strategically important, they cite

inefficient processes, insufficient data and the lack of collaboration between business and IT groups as the leading causes of risk across the enterprise. Specifically:

- » 58 percent use mostly manual methods to monitor identity controls. Many identity and access management tasks are still dependent on multi-step processes and paper-based workflow, driving business costs up and organizational efficiencies down.
- » 87 percent employ a decentralized identity compliance strategy. An overwhelming majority of companies focus compliance efforts on applications, departments or locations in lieu of centralized policy enforcement and access review procedures.
- » 51 percent take a detective (or reactive) approach to identity-related compliance issues. Most organizations still don’t know a compliance breach has occurred until after the fact.

When you consider the hundreds of applications and thousands of users in most large enterprises, there’s no underestimating how difficult it is to keep track of all the moving parts. Exacerbating these issues is the inherent disconnect between business and IT groups – folks who depend on each other to get their jobs done, but who “speak” very different languages representing very different agendas.

Although the Ponemon findings show that the responsibility for identity compliance is shared across business, IT and audit/compliance groups, collaboration among them is acknowledged as very weak. In fact, 42 percent of respondents say that

collaboration rarely occurs, while another 23 percent say it never occurs. In addition, more than 42 percent believe the primary barrier to collaboration is the lack of technical knowledge or domain expertise held by audit and compliance personnel, a significant data point given the level of influence this group has over corporate compliance initiatives.

So what are C-level executives to do?

Companies must focus their identity risk management efforts on the information assets that represent the most value – and potential liability – to the business. The only way to do this is by implementing a solution that provides meaningful business context for the volumes of low-level identity data (user access privileges and audit logs) generated by diverse IT systems and applications. This business context must provide rich, multi-dimensional views of identity data that combine information such as job functions, asset risk and compliance policies with technical data mined from the IT environment – in effect, a single data model to help organizations centralize, filter and interpret critical compliance information, and bridge the communication gap between business and IT groups.

Take the example of Joe Smith, the likeable finance guy who’s worked at your company for years and has earned the trust and admiration of pretty much everyone around him. Over time, and across multiple job roles, Joe has accumulated access privileges to countless sensitive business applications. Some of these are required to do his job, some are not. Does your organization have a way to track which access privileges Joe has acquired and to tie them back to specific business systems? Can you tell which ones represent a separation of

duty conflict, potentially violating a policy that says Joe shouldn’t be able to set up new vendors, process invoices and cut checks? Do you have any way of knowing how often Joe’s privileges are getting reviewed by upper management, and by whom? And finally, can you quantify how much risk the sum of these factors represents in the context of your larger financial organization? Or your company as a whole? Would you be surprised to find out one day that Joe had transferred a total of \$50,000 into various personal bank accounts? You shouldn’t be. The risk is real, and it’s being put to the test every day.

According to Ponemon survey results, companies face a number of key barriers in quantifying risks like Joe. 42 percent of respondents say the data they need to assess risk is difficult to obtain, 41 percent say they lack the appropriate tools to track and assess such risks, and another 21 percent say they have no way to assign tangible risk values to technical resources – bringing us full circle to the issue of business context, and how important it is in mitigating the risks associated with user access privileges and activities.

It’s not difficult to understand that a reasonable amount of identity risk is appropriate and necessary in every business, regardless of how many users or sensitive information systems comprise an organization. The key is how well companies manage these risks by implementing strong and consistent controls over who has access to critical applications and data – and what they do with it. Savvy companies will seek a cross-disciplinary management approach that involves business, IT and audit groups in the definition of common goals and compliance metrics, leveraging risk-based analytics and a

centralized view of identity data to proactively prevent, detect and correct identity risks. ■

## SailPoint Technologies

SailPoint is dedicated to helping organizations achieve continuous compliance, strengthen internal controls and strategically manage risk associated with user access to sensitive applications and data.

## SailPoint Compliance IQ

SailPoint Compliance IQ is an innovative identity risk management solution. It automates and streamlines compliance processes including policy enforcement, access certification, and activity monitoring. Compliance IQ improves audit performance, lowers the cost of compliance and reduces the risk of privacy breaches.

## Contacting SailPoint

Please contact us either online, at [www.sailpoint.com](http://www.sailpoint.com), or via phone at 512.346.2000.

Mark McClain is the CEO and Founder of SailPoint Technologies. He drives the vision and overall business strategy for SailPoint. Previously, he was founder and president of Waveset, where he helped establish the company’s industry-leading position in the identity management space, including 250 percent revenue growth year over year for three years. Following the acquisition of Waveset by Sun Microsystems, Mark served as vice president of marketing for Sun software. He has diverse experience in international sales and marketing with Hewlett-Packard, IBM and Tivoli Systems.

