IDC BLOG
Sponsored by: SAP

Key Business Stakeholders Play Critical Role In Solving Complex Data Security, Regulatory Compliance Issues, Study Finds

December, 2018

Written by: Robert Westervelt, Research Director, Security Products Group, IDC

Enterprises undergoing digital transformation (DX) are eliminating data silos and implementing advanced analytics to get actionable insight into the data proliferating across the organization. These businesses are maximizing resources and operational agility by integrating supply chain, HR and other ERP applications. Several ongoing IDC studies are documenting compelling results, but they are also uncovering security and compliance complexities that require people and process improvements to fully realize the DX benefits.

These security and compliance complexities have driven a new approach to DX and is why SAP's approach to the Intelligent Enterprise ensures that organizations are enabled to bridge the siloed enterprise applications by orchestrating process and technology to support advanced analytics across data sources. However, process and technology alone won't address security and privacy challenges. Information Technology (IT) security teams must enlist operations and lines of business personnel to address gaps often found during the DX journey. Advanced analytics is helping gain untapped value out of corporate data, but data and application stakeholders must play a key role in security and privacy.

The security of business applications in the cloud requires security teams to engage with business analysts and data specialists who have the most visibility. Enterprise security and data management specialists report to IDC that ensuring security, integrating cloud resources with existing IT infrastructure, and legal requirements/restrictions are the top three challenges they encounter while adopting multiple cloud environments and maintaining on-premises resources.

Security is viewed as a significant hybrid cloud adoption challenge. It also is the primary reason – even more than cost and productivity – for reducing traditional on-premise IT infrastructure in favor of public cloud and private cloud resources, according to IDC's Data Services for Hybrid Cloud survey of more than 400 IT security and line of business personnel. The technology adoption is compounded by the need for businesses to take measures in response to the European Union (EU) General Data Protection Regulations and increasing public concern over data protection and privacy. More than 64% of those surveyed cited regulatory compliance as challenging or very challenging across their hybrid environments, and nearly 63% experienced significant pain ensuring data rules meet corporate governance initiatives.

The survey results indicated that today 77.4% of enterprises currently run some workloads on traditional on-premises IT infrastructure, and the survey findings also suggest the number will be cut by half by the end of 2019.

Adopters of SAP Intelligent Enterprise suite have the added benefit of increased agility and can also rapidly change and improve outcomes against disruptive competitors. However, one of the most powerful benefits is enabling the security team to shed the reactive security strategies applied to previously siloed resources. Security teams can take advantage of underlying architecture improvements and take a data-centric security approach with key operations personnel and business stakeholders.

Enterprise buyers often consider technology improvements to bolster security and privacy, but IDC research has found that people and processes are often last to be addressed. The irony is that people are often not engaged, which can lead to policy and process failures that may pose the most significant obstacles to mitigating risk. Nearly 62% of survey respondents cited the challenge of addressing data quality issues and ensuring data quality, requiring assistance from data owners. And 58% said being able to locate and access data from different sources was a key requirement, necessitating security to work closely with stakeholders to understand critical workflows requiring security improvements.

There are countless examples of organizations overcoming policy and process failures by engaging key business stakeholders. The Chief Information Security Officer (CISO) at a global manufacturer engaged line of business IT and operations personnel and cited significant improvements in the company's security posture following the recent migration of the company's ERP applications and data on a single instance of SAP HANA S4 with Business Warehouse and Business Intelligence. In an interview with IDC, this CISO said that the newly adopted architecture, hosted in a private cloud and used globally by about 2,700 end users, enables business analysts to securely aggregate and orchestrate various data sources into a single data source for analysis.

Key stakeholders assisted in a two-year effort to correct corrupt or inaccurate records, standardize, and classify data across various data stores as part of the aforementioned project. SAP's Governance Risk & Compliance solutions and services helped establish role-based access control and automated change management processes, the CISO told IDC. "If an employee moves to a new job, the changes are automated and there's not a lot of administrative work," he said. "It does the aggregation and the orchestration of various data sources securely and provides my team with the telemetry to address potential threats while enabling business analysis to conduct ad hoc queries against internal and external data sources."

More enterprises are expected to undertake similar projects. Today 77.4% of enterprises currently run some workloads on traditional on-premises IT infrastructure, and the survey findings suggest the number will be cut significantly by the end of 2019. The following action items can help make the transition smoother by minimizing disruption and applying controls to protect the most sensitive data.

» **Establish Digital Trust and Optimize Governance:** Engage and empower key personnel as advocates to instill security into the culture and leverage data protection and privacy as a competitive advantage. Mitigate compliance risk and build trust into the culture of the organization and the foundation of operations. Once critical data assets are identified and mapped to access rights and existing workflows, identify gaps, eliminate siloed security investments, and consider implementing centralized data protection and privacy controls, where possible, to maintain consistency.

- **Practice Continuous Assessment and Remediation:** Existing monitoring and alerting solutions should be coupled with policies and processes to gain full situational awareness over the status of ongoing projects, incident response activities, and compliance audits. Procedures should be in place for monitoring for emerging threats to business systems and timely testing and deployment of security updates. Engage impacted stakeholders to help existing security technologies and ensure they are properly deployed and securely configured and maintained to protect critical assets. Processes must assist security teams to rapidly investigate and address security incidents and recommend ways to prevent reoccurrence through updating and more effectively communicating policies, processes, and technology improvements.

- **Modernize/Optimize Systems:** Organizations must assess existing policies and processes and plan for changes when adopting new technology or modernizing existing investments. This is especially important when infrastructure is impacted. Evaluate security solutions to ensure they integrate with existing infrastructure. Gauge the extensibility of the security product to determine whether it can adapt to emerging technologies without costly retrofitting. New solutions should come from a provider that demonstrates commitment to data protection and privacy by design and by default.

About the Analyst

Robert Westervelt, *Research Director, Security Products, IDC*

Robert Westervelt is a Research Director within IDC's Security Products group. He provides insight and thought leadership in the areas of cloud security, mobile security, and security related to the Internet of Things (IoT). Rob is also responsible for research and analysis around a wide range of evolving security markets, including endpoint security, security and vulnerability management (SVM), and identity and access management (IAM).

IDC Custom Solutions

IDC Corporate USA

5 Speen Street
Framingham, MA 01701, USA

T 508.872.8200

F 508.935.4015

Twitter @IDC

idc-insights-community.com

www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.