SAPinsider

Secure, Vigilant, Resilient

How Companies Can Keep Pace with the Evolving Threats of Modern Business

Jeff Lucy
Director
Deloitte & Touche LLP

Bill Smith
Senior Manager
Deloitte & Touche LLP

Despite heightened attention and an unprecedented level of security investment from organizations, the number of cyber incidents and their associated costs continue to rise. Increasingly sophisticated hackers cause some to question whether security is even possible in today's rapidly evolving landscape of cyberattacks.

The very innovations that drive business growth and value — such as the proliferation of sensitive data and the mobile access that employees often have to it — create cyber risks that, if not checked, can outweigh the business benefits the organization is seeking. To stay secure, vigilant, and resilient in a rapidly evolving landscape of cyber threats, companies need to identify the top risks they face and develop a sound cyber risk program that includes software such as SAP solutions for governance, risk, and compliance (SAP solutions for GRC).

Secure

Traditional security controls, preventive measures, and compliance initiatives tend to consume the majority of companies' investments in cyber risk management, and this investment will either need to continue at current levels or increase. Companies should build a business-centric access and data protection program that appropriately balances the needs for speed, scalability, and sustainability.

SAP Access Control can help companies understand areas of sensitive data access, enable stronger access controls for areas of high sensitivity, and provide additional approval controls. SAP Process Control can help a company manage and monitor its controls environment, specifically internal controls that handle areas of sensitive access as well as recertification of controls. SAP Regulation Management by Greenlight, combined with public information sources, can provide companies with insights around what is required to be properly secured to enhance their security profile.

Vigilant

Efforts to be vigilant start with a solid picture of what a company needs to defend against. Knowing a company's specific business risks as well as the larger threat landscape within its industry is an important starting point. Effective cyber vigilance requires robust monitoring of infrastructure, applications, and users.

SAP Fraud Management and SAP Access Violation Management by Greenlight can detect anomalous business transactions embedded in mass amounts of activity that could indicate a potential compromise of a user's credentials or access abuse. SAP Regulation Management by Greenlight can consolidate inputs across the technology landscape to provide consolidated perspectives on the overall vigilant posture of the organization.

Resilient

Technology teams handle many day-to-day, routine security events, but some incidents may become serious business crises. Being resilient means having the capacity, at a moment's notice, to contain the damage and mobilize the diverse resources needed to decrease its impact, including direct costs and business disruption as well as reputation and brand damage.

SAP solutions for GRC help companies manage and expand their existing crisis management programs. With SAP Risk Management, companies can manage areas of potential impact and gain insight into risk exposure. Companies can assign hard-dollar figures to areas of risk, allowing them to better quantify the potential impact.

Learn More

To learn how Deloitte is helping organizations strengthen their cyber risk programs by incorporating the capabilities of SAP solutions for GRC, visit **www.deloitte.com/sap** or email us at **jlucy@deloitte.com** or **billsmith@deloitte.com**.

Reproduced from the Oct ▪ Nov ▪ Dec 2015 issue of *SAPinsider* with permission from its publisher, WIS Publishing | SAPinsiderOnline.com