



Aberdeen *Group*

Best Practices in Security

Governance

Managing Risk is Central to Security Performance for this Financial Services Company

Business Challenge

This large financial services company operates many lines of business. In a very competitive market, the business pressures include mergers and acquisitions, divestitures, regulatory mandates, changes in financial markets, and the management of risk.

As a global company, this organization's usage and practices of technology are very similar to some of the larger technology solution providers. With its own development organizations, business lines and organizational challenges, this company must optimize a balancing act when it comes to its security programs: manage risk for each business unit while implementing consistent security risk management programs across all IT operations.

Strategy

This firm has mature policies and standards that reach down to the product and application level. The standards have led the firm to footprint-standardized systems, networks and software solutions that are implemented throughout the organization. Using a formal change management program, the organization also implements compliance standards, including the handling and disposition of information, whether it's transported physically or electronically.

To respond to its business pressures, the company decided it required the use of centralized repositories, customizable software, workflow and inventory capabilities, along with technical and business risk management thresholds and processes to better manage acceptable risk levels across the company and its business lines. So, the company selected solutions from Archer Technologies to automate its risk management programs.

Best Practices in Security: Governance

Company Name

Financial services

Solution Provider

Archer Technologies

Business Challenge

Mergers and acquisitions, divestitures, regulatory audits, financial markets and risk management

Strategy

Implement business and technology risk management programs that are flexible enough for business lines while able to accommodate corporate-wide standards, procedures, data, and knowledge

Value Achieved

- Risk management programs for controlling and managing "information risk"
- Risk management programs for controlling and managing all other aspects of security for networks, systems, databases, access, etc.
- Efficient methods to collect, analyze, categorize, track, and report security information



Deployment Experience

After conducting evaluations, selecting the Archer solutions, and conducting pilots, this firm rolled out its initial implementation during the past year. Since then, the company has deployed more than 65 custom modules used to help encapsulate compliance with its information security standards and to compare its critical metric thresholds against actual conditions occurring locally. To date, the program has been a success, largely due to the ease with which the custom modules can be created, tested, and deployed in such a complex environment.

Results

The results have enabled the company to track inventory and remediation data, reminders, and attestations, as well as automate risk assessment procedures, workflow, and prioritization methods to resolve and maintain security profiles based on risk levels established for both business and technology reasons. The Archer solutions, used to align compliance with internal security and risk standards, are also being counted on for managing external audit and regulatory requirements.

Lessons Learned

The company has learned that governing its security programs requires that it place more emphasis on the practices, standards, data and knowledge that come from managing risk. As a result, the company has learned that governing its security programs requires it place more emphasis on ensuring that all components of information security (e.g. systems, processes, risk assessments, and holding people accountable) are readily available and maintained in real time. Most important, as information security becomes truly ubiquitous, the company depends increasingly on efficient methods for collecting, inventorying, categorizing, analyzing, reporting, and remediating all these components.

Future Outlook

This organization is planning to implement formal information risk management programs this year to accelerate a formerly “asset-based view” into what the real assets are: the company’s sensitive information, customer data, and information about business partners and suppliers.

Aberdeen Conclusions

This company’s metrics, practices, and performance results qualify it for inclusion in the top six, and it’s headed for further improvement of its security performance results. The opportunity going forward will be to align the actions and results from its security programs, especially across independent IT organizations, around the central theme of managing risk. The organization may want to consider adding additional controls on information that will optimize its performance in accordance with the company’s standards, practices and procedures.