
Executive Summary

Business operations must be available, often 24/7, and this entails the use of networks, devices, computing platforms, data storage systems, e-mail, the web, and information. However, not all enterprise IT resources are under enterprise control. The ability to maintain auditable control and security for IT infrastructure is becoming more difficult and more important. Enterprises are struggling to balance flexibility and agility with managing the risk that comes with unfettered access to information among employees, customers, business partners, and suppliers. Further, government regulations covering financial data and customer information are complicating this balance between business agility and business risk.

Similarly, the sales order database, credit, and internal controls database should serve the authoritative source for customer self-service initiatives. Organizations are seeking tools to be able to corroborate the location of core data, changes to the data, and ascertain the exposures in their databases, and their underlying operating systems. Solutions to assess database vulnerability management and information risk management can harden IT databases, and test and validate application and configuration faults

Aberdeen's research shows that best practices for security in an environment involving less direct control means firms have to dramatically improve processes and procedures to verify the security of the interconnected networks, systems, applications and underlying data throughout their value chains to operate their missions and business functions. Without the correct balance, Aberdeen conservatively estimates that *industries are missing the mark on customer loyalty, repeat orders, top-line revenue, cost savings, and profits each year through inefficient alignment and automation of information access for core business operations.*

A reality of information security is that many firms don't want to paint red targets on their backs by divulging their practices, out of fear that any additional information made available to hackers and thieves will negatively impact them. While preserving anonymity, Aberdeen is committed to improving the results that other organizations not operating at best-in-class levels can achieve.

Recommendations for Action

Aberdeen recommends that organizations take the following actions to improve security for information and access:

- Link business drivers and pressures with automating information access;
- Appropriate, business-focused performance metrics to drive results faster than traditional IT-selected security performance metrics will;
- Map business performance metrics with those that can be monitored;
- Foster a corporate culture and business processes oriented around the end user; Consider implementing the practices of the profile organizations; and
- Build a leadership council that includes business leaders.

The difficult part about security is making sure it's aligned with the organization's needs, business missions, and external regulatory pressures. Companies that are able to do this can bridge the gap between laggards, industry norm and Best in Class. In short, companies implementing best practices for information and access are more successful in dealing with business pressures impacting their organizations and in overcoming challenges. By turning the traditional security model inside-out – focusing on the data and its business value – enterprises can balance information access and the inherent risks.

Turning Traditional Security Model Inside-Out Pays Big Dividends for Financial Services Firm

Business Challenge

With more than \$24 billion in assets under management and more than 1,000 business customers, this financial services firm delivers a wide range of services, including electronic processing, investment services, electronic payment processing, credit services, funds transfers, and settlement services.

Operating as one of the largest service providers in its sector of the financial services industry, this company is under intense pressure to deliver assurances to customers that their data and the company's corporate data and processes surrounding the safety of this data remain sacrosanct.

Strategy

The company overhauled its approach to security several years ago by turning the traditional security model inside-out. Instead of implementing security solely from the periphery and working inward, this company decided to focus on data and its business value and work outward. This allowed the company to focus its information security risk management efforts on the most critical assets and allocate the most appropriate resources and technology.

As part of this effort, the company decided to tackle its biggest challenge of all: identifying where its critical data resides, the value of the data to the business and its customers, the workflows that operate on the data, and the behavior associated with access to the data.

The company integrated the security function into the business units to improve results faster, overhauled its metrics for IT security, and focused its security programs on managing risk across its business operations and enabling technologies. During the evolution of its security program, the company deployed a wide range of vulnerability assessment technologies to identify weaknesses. As part of this evolution, the firm decided to automate security scanning, vulnerability assessment, and remediation for where most core data resided: in databases.

Best Practices in Security: Information and Access

Company Name

Financial services company

Solution Provider

IPLocks

Business Challenge

Maintain customer faith that data is protected and safe

Manage regulatory audits

Strategy

Turn security inside-out by focusing on the core data

Overhaul the security function and focus it on managing risk at the business unit level

Values Achieved

- Reassured customers that their data is safe
- No shutdowns to data flows
- Vulnerabilities and risk-behaviors curtailed
- Highly unlikely to become a poster child for data leakage reported in the media

Solution Deployment Experience

Using solutions from IPLocks, the company has been able to verify the locations of core data, the vulnerabilities in its databases and their underlying operating systems, and the changes to data. The company is using alerts for conditions that exceed its risk thresholds, while ensuring that configuration mistakes and security vulnerabilities in the databases are fixed. In addition, the company has been able to identify and eliminate inappropriate privilege conditions, authorized and unauthorized access to data, and suspicious behavior regarding its most valuable IT assets: its data and customers' data.

Results

The use of the IPLocks solutions has enabled this firm to harden its databases and avoid privilege-race conditions that tend to lead to fraud and theft, while avoiding any undue performance loads that would be noticeable to business operations. The solutions are being used at granular-levels that make a difference, including database queries, database builds, database patches, privileged operations accessible to database administrators, database schemas, and database metadata.

In addition, the company's risk-based approach to security, utilizing the OCTAVE methodology from Carnegie Mellon University, has enabled it to evangelize the value of information security risk management throughout the organization because it bridges the gaps between the business lines, the finance organization and the technology controls.

Lessons Learned

In this day and age of data privacy, publicity about data-leakages and corporate value, one of the primary lessons this company learned is that it was correct to undertake two fundamental changes in the way it approached security: (1) Start where the valuable data is, and (2) Make security usable to the business by managing it as a risk underwriting and transfer activity focused on the core data assets of the organization. In addition, the company learned that security awareness is critical to results: once everyone understands his or her role, it turns in performance results much more rapidly.

Future Outlook

This company is well on its way to security governance now that it has all the pieces in place to balance the acceleration of access to information and the inherent risks that accelerating access poses to the organization. Instead of focusing on what the security frameworks say, this company is focusing on how to achieve results.

Aberdeen Conclusions

Despite the large foray into network security that grips most firms, this company is proof that, after network and infrastructure security, the next rung up the security value ladder is information and access. While it's focused on information and access, this firm is also accelerating quickly into security governance to achieve its business objectives.

AberdeenGroup, Inc.
260 Franklin Street
Boston, Massachusetts
02110-3112
USA

Telephone: 617 723 7890
Fax: 617 723 7897
www.aberdeengroup.com

© 2005 **AberdeenGroup, Inc.**
All rights reserved
September 2005

The information contained in this publication has been obtained from sources Aberdeen believes to be reliable, but is not guaranteed by Aberdeen. Aberdeen publications reflect the analyst's judgment at the time and are subject to change without notice.

The trademarks and registered trademarks of the corporations mentioned in this publication are the property of their respective holders.

Founded in 1988, **AberdeenGroup** is the technology-driven research destination of choice for the global business executive. **AberdeenGroup** has over 100,000 research members in over 36 countries around the world that both participate in and direct the most comprehensive technology-driven value chain research in the market. Through its continued fact-based research, benchmarking, and actionable analysis, **AberdeenGroup** offers global business and technology executives a unique mix of actionable research, KPIs, tools, and services.