Research Brief

Aberdeen Group
A Harte-Hanks Company

June 18, 2007

Financial Supply Chain Transactions: The Rising Importance of Information Protection and Secure Connectivity for Data Exchange

Rising Complexity of Financial Supply Chain Transactions and the Role of Data Security

With the growing complexity of today's global supply chains, the accompanying financial transactions are also growing in both volume and complexity. This growth is placing more pressure on financial institutions to support secure data exchange for their clients.

Increasing amounts of sensitive commercial data need to be securely moved to enable corporations to manage their procure-to-pay and order-to-invoice processes on a global basis. In fact, Aberdeen research into corporate use of on-demand platforms for procure-to-pay and order-to-invoice processes finds that **data security is the top concern** of the 180 corporations studied, cited by 64% of respondents[1]. In addition, 60% said they were also very concerned with how to integrate the data back into their own systems.

Concern about end-to-end data security also extends to the financial community. Data security remains an issue of key concern for 92% of financial institutions that Aberdeen surveyed in May 2007.

A Call for Secure Information Transfer

Secure information transfer with low IT costs is what corporations are seeking today. This is particularly important because of the increased volume and detail of data being shared electronically between business partners. Banks today are required to satisfy the need for creating secure flows of financial data, end-to-end financial supply chain visibility, and – a demand by the leading corporations – real-time status tracking of financial supply chain events. Aberdeen research finds that large enterprises – whose business operations are often global – are very concerned with the lack of appropriate technology systems to manage their financial processes and risk exposure.

The focus on a secure environment for financial supply chain transactions has been heightened in light of numerous security breaches reported by financial institutions in recent years. These breaches have been well publicized by the media. To retain and expand their relationships with corporate clients, banks and other financial institutions need to ensure they have created a fully up-to-date data exchange environment for payments, receipts, financing, and more.

Banks' Role in the Move to Increased Financial Automation

Aberdeen studies on supply chain finance report that 55% of companies now believe that their manual-intensive financial processes are too burdensome: this finding highlights the lack of financial supply chain automation that often opens the door for

[1] *The On-Demand Tipping Point in Supply Chain Benchmark Report*

risk events (e.g. data errors, leaks, etc). This alarming situation reported by corporations can be sometimes eased with the help of their financial institution partners – in the past several years, banks and other financial institutions have understood the importance of transaction processing and connectivity technologies for their clients' long-term success and have started offering their clients a variety of technology enablers to automate financial supply chain transactions.

For banks, it is absolutely critical to ensure the security of their customers' financial information that is being moved through their technology platforms internally and exchanged with clients and other outside parties. Some financial institutions have already upgraded their technology capabilities to increase the security of their clients' data flows. Banks that have not yet done so face several risks that may inflict both immediate and long-term damage on the institution:

- **Reputation risk**: Because data concerns rank high for the corporates, a security breach would seriously damage the bank's reputation. As competitors are getting ahead with new financial products and better enabling technologies, lack of activity on this front can erode a bank's reputation in both its customers' and competitors' view.
- **Operational risk**: Manual management of key bank-to-corporate as well as internal bank processes can lead to critical errors (e.g., duplicate files being delivered and processed, multiple versions of documents – no "single version of the truth", processing delays, etc.)

To estimate some of the challenges, strategies, and key concerns of financial institutions as it relates to data security, Aberdeen conducted a survey of 24 financial institutions in May 2007. The secure exchange of data is becoming increasingly important for these institutions to deliver innovative financial services and sound transaction processing environments. The next section shares the results of this survey.

JPMorgan Chase on information security:

√ David Matthews, Senior Technology Director at JPMorgan Chase, says that the bank takes information security seriously and targets the following areas for continuous improvement: securing digital signature with multifactor authentication, enhancing permissions technology, checking fraud measures, enhancing disaster recovery provisions, securing e-mail, strengthening the transaction processing infrastructure and internal security. "On a daily basis, an enterprise-wide Incident Response Team works to identify and address any vulnerabilities in accordance with JPMorgan Chase's IT Risk Management standards, and manage any security issues that may arise. Internal audits and vulnerability assessments are conducted on a regular basis, plus regulatory oversight of IT applications and e-business infrastructure is conducted by both an internal Information Security team and independent third parties" – says Mr. Matthews

Financial Institutions' Growing Concern about Information Security

Data protection and information loss prevention in a financial institution's internal and external processes are mission-critical issues. The results of the Aberdeen survey show that data protection and information loss prevention are of great concern: **64%** of respondents reported this as a **high priority for improvement** at their institution, and **28%** said it was **among their top 2 priorities** overall. Just 8% said that it was not a key priority for their organization.

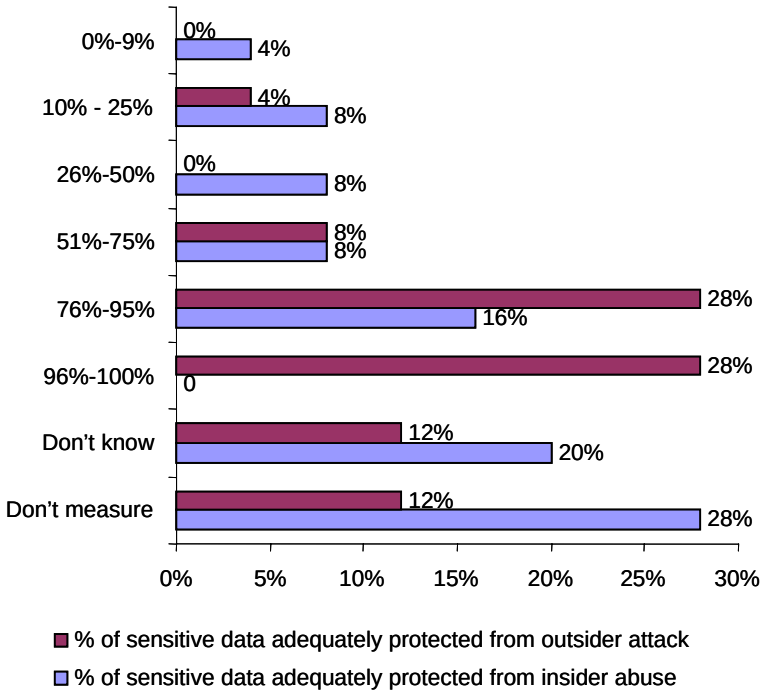
When asked about their top 2 strategic actions to improve data protection, respondents overwhelmingly said those actions were to:

⇒ Identify and protect sensitive data — **88%**

⇒ Deploy end-to-end data protection — **44%**

The survey revealed certain alarming results on the current state of information protection practices among the institutions participating in the study. Figure 1 below shows the current levels of protection from both insider and outsider attacks:

Figure 1. Percentage of Financial Institution's Sensitive Data Adequately Protected from Insider and Outsider Attacks



Source: Aberdeen Group, June 2007

As evident from the Figure 1, few participants (less than one-third) could confidently state that over 95% of their sensitive data is adequately protected from outsider attacks; and protection from insider threat is far less than that. Especially alarming is that one-fifth of respondents do not measure this statistic at all!

Given the situation reported in Figure 1, it is important to note that a large percentage of respondents said that these metrics had actually improved over the past two years. This shows that even though some progress is being made in securing data, financial institutions are still far from being fully protected from internal or external data threats (Table 1):

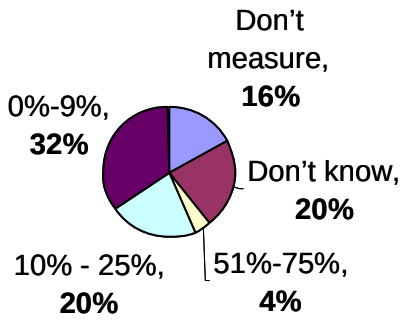
Table 1. How Has This Metric Changed Over the Past Two Years?

	% of sensitive data adequately protected from insider abuse	% of sensitive data adequately protected from outsider attacks
Remained Same	24%	16%
Improved	40%	64%
Gotten Worse	12%	4%
Don't know	16%	16%

Source: Aberdeen Group, June 2007

Financial institutions in the survey spend the following percentage of their IT budgets specifically on data protection (Figure 2):

Figure 2. % of IT Budget Spent on Data Protection



Source: Aberdeen Group, June 2007

Even though most institutions dedicate a portion of their IT spend to information loss prevention, study participants still report the occurrences of data leaks: over the past year, only about **60%** of institutions stated they had not experienced any data loss and had not had any financial losses associated with such data leaks. Surprisingly, about **one-fifth** of companies said they either did not know whether their institution had had data leaks or did not measure the estimated financial losses. **8%** of respondents reported that they had experienced some type of data loss and the ensuing financial losses (of varying magnitude).

When asked about the dynamic over the past year, less than a quarter of companies reported that data incidents and impacts have improved. As Table 2 shows, most companies reported that results have stayed the same.

Table 2. How Have the Security Metrics Changed Over the Past Year?

	# of data loss / data leak incidents	Financial loss associated with data loss/ data leak incidents
Remained Same	44%	44%
Improved	16%	24%
Gotten Worse	8%	12%
Don't know	32%	20%

Source: Aberdeen Group, June 2007

Banks Increasing Focus on Financial Supply Chain Capabilities and Information Security

Financial institutions must place a renewed focus providing transparent and visible, yet highly secure, financial data flows for themselves and their customers. Secure information flow is a critical foundational element for financial institutions to remain competitive in the expanding market of financial supply chain services and supporting technology offerings. Enhancing the security of the connectivity environment decreases fraud and errors that could potentially harm the institution.

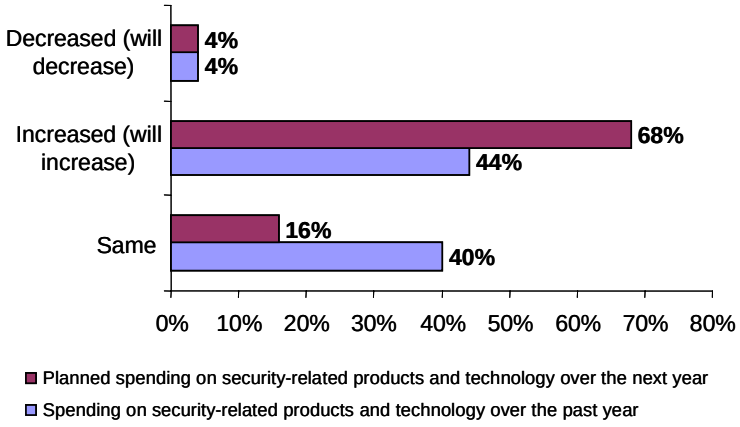
As revealed by the Aberdeen study, financial institutions still need to make improvements in their ability to process financial transactions in a secure environment. The data from this study also show that the financial services provider community is realizing the need to act, as indicated by a large percentage of respondents that plan concrete steps to enhance their security-related products and technology to improve data security at their organizations (Figure 3):

Checklist for Evaluating Solution Providers:

Items to evaluate when selecting a solution provider for your bank-to-corporate connectivity capabilities:

- √ Vendor viability and industry understanding
- √ Protocol management capabilities
- √ Mapping and translation capabilities (including Financial Services Industry Standards Management)
- √ Automated scheduling / event triggers (to allow unattended transfers)
- √ Robustness of security capabilities, including encryption, firewalls, multi-factor authentication, etc
- √ Scalability: the ability to handle very large files

Figure 3. Spending on Security-Related Products and Technology over the Past Year and Planned Spending over the Next Year



Source: Aberdeen Group, June 2007

Financial institutions must continue enhancing the security of their financial transaction processing environment and aim to achieve these goals for the long-term benefit of their clients:

- Alleviate clients' internal IT constraints by providing robust technology infrastructure and support for financial data interchange
- Alleviate security concerns by providing a more secure multi-party environment for managing financial information

For more information on this or other research topics, please visit www.aberdeen.com or contact: Jason.Hobart@aberdeen.com

Related Research

Technology Platforms for Supply Chain Finance Benchmark Report (March 2007)

Thwarting Data Loss Benchmark Report (May 2007)

Author: Viktoriya Sadlovska, Research Analyst, Global Supply Chain/Supply Chain Finance (Viktoriya.Sadlovska@aberdeen.com)