Data Security.

Mitigating the Strategic Risks of Identity Theft in the Broker-Dealer Environment

An executive briefing on the hidden threats associated with protecting personally identifiable information, and how leading organizations are uncovering and addressing them

Broadridge®

Introduction

Senior executives of financial services firms are demanding that information security and data protection strategies advance beyond their traditional enterprise-wide focus.

Their charge: to broaden the scope of security to include inter-organizational measures that protect information shared with vendors, partners and customers.

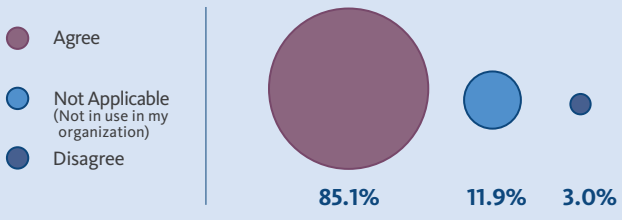
This broadening of executives' perspectives on security is just one finding to emerge from a study of how broker-dealers and other financial services industry executives are responding to fundamental landscape changes in these areas:

- Competition
- Regulation
- Technology
- Threats
- Changes in information distribution strategies and channels

According to a Broadridge survey of over 200 executives in broker-dealer institutions (conducted during the first two weeks of April 2011), over 85 percent of respondents reported that data security and the protection of personally identifiable information (PII) are receiving significant senior executive scrutiny.

Why is the executive suite increasingly interested in data protection? It's because the stakes are rising as their companies struggle to manage growing volumes of sensitive corporate information in increasingly decentralized, distributed, outsourced and complex environments.

QUESTION: Data Security and PII protection are priorities for my organization's senior executive leadership



Survey conducted in April 2011.

IN THIS REPORT WE WILL:

- Explain how key industry shifts and a threatening landscape are affecting the broker-dealer community
- Offer senior-level executives a strategic context within which to make effective decisions to mitigate risks

Our review of the survey data on current attitudes and activities in the sector, combined with our analysis of emerging best practices, has strengthened our belief that broker-dealers are under increasing pressure to develop:

- Extensive, integrated and automated enterprise-wide data protection strategies
- Interorganizational conventions for mitigating data-loss risks among customers, partners and third-party providers

The consequences of ineffective data protection, especially those associated with PII, can be severe. Improperly managed, such data loss represents a strategic risk to organizations. Even "potential" vulnerabilities can conceivably cause significant reputational, financial and operational damage.

Recent high-profile breaches in the financial services sector have elevated the intensity of public debate on protecting PII within the industry, among regulators as well as the investor community.

© 2011 Broadridge Financial Solutions, Inc. Broadridge and the Broadridge logo are registered trademarks of Broadridge Financial Solutions, Inc.

A Changing Environment

Organizations in most industries have taken steps to protect highly sensitive information about customers, business strategy and organizational operations. Many have focused on putting data in secure locations they manage and are thinking about other strategies to keep unauthorized individuals from accessing it. This has been the strategy of many companies in the broker-dealer community as well.

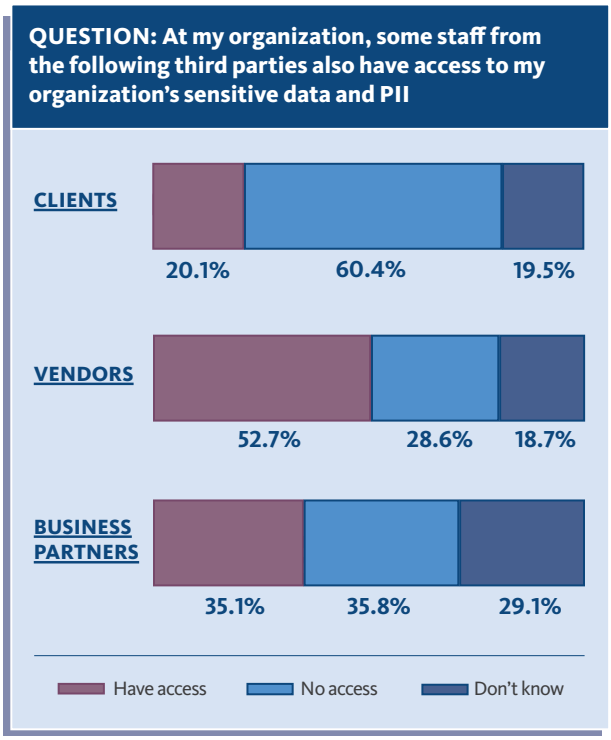
BUSINESS PROCESS EVOLUTION

New competitive pressures, however, have prompted institutions to explore new business models that reduce cost and improve speed while enhancing response to customers. These efforts have translated into expanded requirements that have changed the risk profile to which data is exposed. For instance, a growing number of broker-dealers must:

- Handle spiraling volumes of data to support new offerings and provide customized services to customers

Survey conducted in April 2011.

- Interact more frequently with customers, partners and vendors through a growing variety of channels (mail, phone, web and mobile devices)



Survey conducted in April 2011.

- Consolidate cumbersome infrastructures that have led to complex, costly data centers. (Often data centers and application resources have been developed in siloed environments to support dedicated service and product offerings.)
- Manage the changing and evolving strategies related to information distribution

Since these activities are outside of the core competencies of some broker-dealers, these organizations often have secured specialized expertise from third-party providers. As a result, growing volumes of data – including PII – are no longer concentrated in centralized facilities exclusively controlled by broker-dealer employees or housed in enterprise-owned facilities.

© 2011 Broadridge Financial Solutions, Inc. Broadridge and the Broadridge logo are registered trademarks of Broadridge Financial Solutions, Inc.

For many broker-dealers, the most sustainable way to respond to these reporting and protection requirements involves automating as many processes as possible, while eliminating manual procedures and their potential for abuse and human error.

REGULATORY SHIFTS

The fallout from the 2008 financial sector crisis ushered in new international, federal and local statutes. The most recent efforts to regulate the financial services market (specifically the Dodd-Frank bill) join the Gramm-Leach-Bliley and Sarbanes-Oxley laws of earlier years in calling for:

- **Increased operational transparency** through more granular and automated reporting
- **Locking down control of consumer data** by demonstrating measures to prevent data loss and restrict access

For many broker-dealers, the most sustainable way to respond to these reporting and protection requirements involves automating as many processes as possible, while eliminating manual procedures and their potential for abuse and human error. Automated processes are easier to monitor, control and audit, and are in a position to provide reporting on demand.

TECHNOLOGICAL DEVELOPMENTS

As rapidly as things have evolved on the business and regulatory fronts, they have been outpaced by advances in corporate and consumer technologies that have altered how organizations behave and how individuals do business.

Technological advances have had a profound impact on the financial services industry and the broker-dealer community. Two developments carry particularly significant implications for managing the data security and PII protection imperatives.

Cloud computing

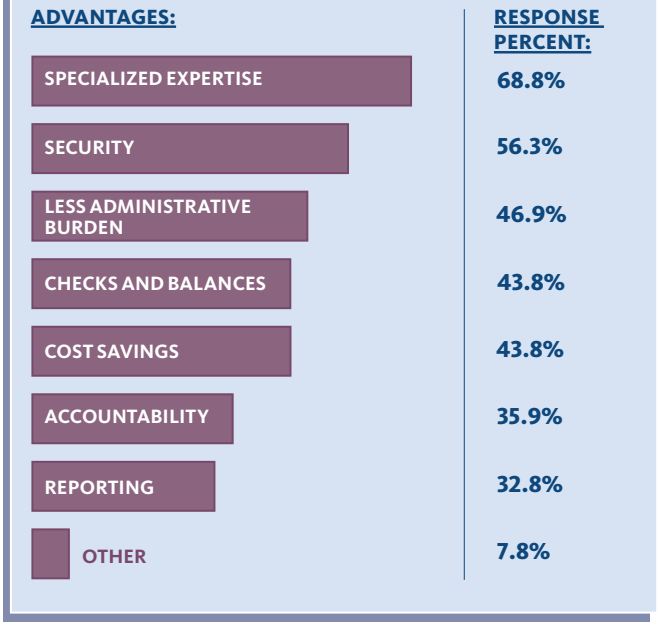
In all its types (private, public and hybrid) and at all its levels (infrastructure, platform and software-as-a-service), cloud computing can help broker-dealers reduce cost, improve time-to-market and preserve a focus on core competencies that generate shareholder value. We have seen rapid adoption of web-enabled applications that give diverse stakeholders much easier access to critical enterprise resources.

However, for many executives, "easy to access" is synonymous with "easy to breach." This has created a conundrum for those who want to gain a competitive advantage by introducing operational efficiencies while also mitigating risks by keeping tight control of data.

There is growing recognition that not all clouds are created equal, and that their different types and implementations imply significantly different security and risk profiles. Indeed, in many situations, the cloud "play" may be the most secure course of action – even for PII assets. The survey respondents even suggest that broker-dealers may have an opportunity to enhance their security posture by tapping into the expertise of vendors who have deep and proven core competencies in security management.

The key to success, as we shall discuss, lies in integrating cloud resources with enterprise-wide security and data-loss prevention strategies.

QUESTION: Working with a third party to support data security and PII protection offers the following advantages over keeping them in-house:



Survey conducted in April 2011.

© 2011 Broadridge Financial Solutions, Inc. Broadridge and the Broadridge logo are registered trademarks of Broadridge Financial Solutions, Inc.

Mobility

In the form of smartphones and tablet computing, mobility is fundamentally transforming the way people interact with each other, their favorite institutions (from banking to retailing), and even their employers.

Mobility has upped the ante on the user experience that customers expect, which consequently has elevated the level of complexity at the end point (where technology touches the user). Mobile data access, therefore, requires intense focus from senior decision makers who seek to win market share while mitigating the risk of losing control of sensitive information.

EVOLVING THREAT AND VULNERABILITY LANDSCAPE

To understand the threats and vulnerabilities to which sensitive information is exposed, we can view them as two distinct drivers:

- **Active attackers,** or people who mean to do your organization harm (often driven by profit motives)
- **Inadvertent acts** from people (employees, clients, partners, etc.) who put your organization in harm's way through error

The profile of active attackers who target enterprises has evolved significantly over the past decade. Gone are the days when attacks stemmed from sophomoric impulses simply to embarrass organizations in highly public forums. It is now believed that most malware – resources designed to break the law – originates from organized crime syndicates based all over the world.

Today's attacks are stealthy, designed to go undetected, and motivated by the desire to monetize cyber-breaches by capturing data to:

- Sell on the black market
- Engage in extortion
- Pursue any range of other criminal activities that yield high profits

Incentives for such attacks are massive. The FBI has estimated that cyber-crime generates as much as $1 trillion a year in illegal profits.

The other face of the active attacker is closer to home – employees who, due to greed or disgruntlement, exploit corporate trust to breach enterprise security measures. The infamous WikiLeaks offers the highest-profile vehicle for those who would purposely expose their organizations to this category of threat.

Passive or inadvertent threats may actually be the source of most data losses. These threats come from people who violate data access controls and policies due to carelessness or ignorance.

These two categories of threat (active and inadvertent) can combine to disastrous effect when unsuspecting employees click on links that allow malicious code to penetrate enterprise cyber-defenses.

...growing volumes of data – including PII – are no longer concentrated in centralized facilities exclusively controlled by broker-dealer employees or housed in enterprise-owned facilities.

© 2011 Broadridge Financial Solutions, Inc. Broadridge and the Broadridge logo are registered trademarks of Broadridge Financial Solutions, Inc.

Action Items
For the Broker-Dealer Community

Today's business strategies rely on the ability to engage with new markets in new ways using a plethora of new technologies. Yet they must be accompanied by equally robust strategies that will mitigate risk and ensure compliance with the regulations, laws and contractual obligations that govern the behaviors of broker-dealer institutions.

For this reason data protection and information security must receive attention and support from the key disciplines of the C-level suite. There are strategic, operational, financial and technological issues that must be coordinated to ensure that:

- Internal processes and procedures are secured
- Interorganizational measures are functioning to protect data as it travels among customers, partners and third-party providers of services

A top-down review of all operations must take place, using a rigorous analysis that addresses these key questions:

- Where does sensitive data, including PII, reside in my organization, and under what conditions?
- Who within my organization has access to this data and for what reason?
- What applications interact with this data, and how is data protection accounted for in their operations?
- Is there an enterprise-wide data protection strategy in place, or is data protection managed department by department?
- Who outside of my organization has access to this data and for what reason?
- Where does this data travel in the course of supporting business operations – both within the enterprise and across the organizational boundaries of:
  - » Customers
  - » Partners
  - » Third-Party Providers
- What are the nature and contractual structure of the above external relationships among organizations that carry sensitive data, including PII?
- How synchronized are the data protection measures among the different parties among whom sensitive data is exchanged?

WHAT TO LOOK FOR

As these and other questions are examined through the perspectives of different C-level disciplines (CEO, COO, CFO, CIO, Compliance, etc.), the resulting strategies and solutions should seek and promote:

- Defined procedures that can generate immediate audit, compliance and forensic reports on demand
- Measures that focus as much on monitoring, rapid response and resilience as on threat detection and prevention
- Measures that have an integrated approach to securing the people, processes and technologies that interact with sensitive data
- Service-oriented protection initiatives that have an integrated perspective on how infrastructure, networks and applications work together to make resources available to end users
- Centralized (i.e. enterprise-wide) policies that govern entitlements and enforce enterprise-wide and interorganizational, role-based access controls to resources that contain sensitive information
- Black- and white-listing initiatives that proactively identify who and what is allowed to touch sensitive information

© 2011 Broadridge Financial Solutions, Inc. Broadridge and the Broadridge logo are registered trademarks of Broadridge Financial Solutions, Inc.

It no longer is sufficient to focus solely on internal process and technological advancements intended to improve security of sensitive data. An overarching perspective must be brought to bear to protect information that flows through the systems of the enterprise, its customers, its partners and its critical technology vendors.

Conclusion

The broker-dealer community's business success increasingly depends on leveraging a set of shared technological resources that requires information of all types, including sensitive PII data, to cross organizational borders. Organizations are creating intimate relationships with customers, partners and trusted vendors to create value chains that generate important shared value propositions.

While this shift is creating many exciting opportunities, it also is changing the risk posture of businesses in fundamental ways. Just as value propositions are being built by synergistic relationships in which the whole is greater than the sum of its parts, executives must ensure that similarly coordinated efforts are undertaken to protect data that flows outside of corporate boundaries.

It no longer is sufficient to focus solely on internal process and technological advancements intended to improve security of sensitive data. An overarching perspective must be brought to bear to protect information that flows through the systems of the enterprise, its customers, its partners and its critical technology vendors.

By using the information and considerations outlined in this report, financial services executives can help to ensure that the new opportunities generated by advances in computing technologies, network services and evolving business strategies are effectively "risk-adjusted" to protect their organizations' reputations, financial resources and long-term interests.

© 2011 Broadridge Financial Solutions, Inc. Broadridge and the Broadridge logo are registered trademarks of Broadridge Financial Solutions, Inc.

With roots that go back more than 40 years, Broadridge is the financial services industry's leading provider of innovative technological and outsourcing services.

Our expertise encompasses every aspect of securities processing and investor communications. Our clients include global banks; retail, institutional and discount brokerage firms; correspondent clearing firms; mutual and hedge funds; investment management organizations; and corporate issuers, all of whom have one thing in common: they look to Broadridge for solutions that help them enhance their performance, increase efficiency, reduce cost and maintain focus on serving clients and shareholders.

For more information about Broadridge's products and solutions, please contact your account manager at broadridgeinfo@broadridge.com.

Broadridge holds the following audits and certifications:
SAS70 Type II and SSAE 16 audits to report on compliance with proper security controls
ISO 9001:2008 Certificate for quality management systems and processes
ISO 27001 Internationally recognized certification for Information and Security Management Systems

©2011 Broadridge Financial Solutions, Inc. Broadridge and the Broadridge logo are registered trademarks of Broadridge Financial Solutions, Inc.