8 Tips for Loan Servicers to Ensure Data Security and Integrity

Sleep better at night by reducing the vulnerabilities of technology’s ‘dark side’

Abstract: Loan servicers today face increasing regulatory and investor pressures to make sure they properly protect and preserve the integrity of their loan records. Data security and data integrity, unfortunately, are two often-overlooked aspects of loan servicing. Failure in either area is a recipe for reputation damage at best, and financial disaster, at worst. The goal of this paper is to provide loan servicers with practical advice on how to ensure you, and your investors, are protected.

By Greg Hindson

Introduction

The global economy’s dependence on interconnected technology has ushered in a new era of organizational and personal vulnerabilities. This paper shall discuss two main areas of technology-related enterprise vulnerabilities – data security and data integrity - and how they impact the loan servicing industry.

In general terms, data security refers to efforts to keep data safe from undesirable parties seeking to exploit it for financial gain. This includes the topics of computer viruses, intrusions and breaches. Data integrity, on the other hand, refers the “quality of correctness” and completeness of information.1

Unfortunately, both areas are often overlooked aspects of managing IT infrastructure. As will be highlighted, the failure to take adequate steps to properly protect information from internal and external threats, or the failure to ensure the integrity of the data essential for the legal protection of assets, are both recipes for financial disaster.

Data Security

Each passing day brings new news of a computer threat or an attack on one of our country’s well-known institutions. The month of April 2009 alone brought us two high-profile breach incidents, one involving the United States’ electricity grid2 and the other involving the country’s fighter-jet project.3

Besides these widely publicized stories, security threats to organizations of all sizes continue to escalate, in part due to the number of remote users accessing corporate networks as well as external parties hacking into systems. It’s also the result of malicious software, known as “malware,” a blanket term that covers everything from viruses and worms to keystroke recorders (“keyloggers”). The effects of malware range from mere annoyances to the stealing

1 Wikipedia definition: http://en.wikipedia.org/wiki/Data_integrity
of confidential information, destroying data, and compromising or entirely disabling systems and networks.⁴

According to Symantec’s Internet Security Threat Report for 2008, malware is a threat that continues to grow, especially for financial services firms in the U.S. There were 1.6 million new malicious-code threats identified in 2008, up 265% from the year before, with financially motivated criminal activity as a recurring theme.⁵

Data breaches also present a critical, growing area of concern. There were 383 cases of data breaches at organizations identified by PrivacyRights.org in 2008, in which more than 83 million identities were exposed. A whopping 29% of all data breaches in which identities were exposed came from financial services institutions.⁶

Loan servicers, of course, are a microcosm of the financial services field. Every day, loan servicers access and update hundreds of thousands of loan records, whether those records are housed in a data closet down the hallway or in a third-party datacenter halfway around the globe. Anyone who has access to consumer loan information, which typically includes a debtor’s contact information, social security number, date-of-birth and other confidential information, owns the liability of protecting it.

In fact, the Federal Trade Commission (FTC) currently enforces several laws that restrict the disclosure of consumer information and require companies to ensure the security and integrity of the data in certain contexts. One is the Fair Credit Reporting Act which restricts disclosure of consumer credit reports except for specified permissible purposes. Another is the Gramm-Leach-Bliley Act which imposes privacy and security obligations on financial institutions. Additionally, the FTC recently testified before Congress that it is supportive of H.R. 2221, the Data Accountability and Trust Act, which would require companies to implement sound data security policies and procedures.⁷

The financial stakes, meanwhile, continue to soar. The average cost of a data breach in 2008 reached $202 per record, a 2.5% increase since 2007, according to a study by PGP Corporation, a global leader in enterprise data protection, and the Ponemon Institute, a privacy and information management research firm. The study examined 43 organizations across 17 different industry sectors. According to the report’s authors, “This finding reinforces the message delivered by leading enterprise IT managers and industry analysts that

The average cost of a data breach in 2008 reached $202 per record, a 2.5% increase since 2007

Source: The Ponemon Institute

¹ http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html

© Copyright 2009, Nortridge Software, LLC. All rights reserved.
organizations must focus on proactively protecting their data instead of relying exclusively on written policies, procedures, and training.”  

**Data Integrity**

Data integrity is an important element of any business. Every day, business managers and the investors backing them make decisions based on macro- and micro-economic data points that are considered to be factual.

Unreliable data, of course, impacts your brand with customers, vendors, management and anyone else who has a vested interest in your enterprise. The criticality of data integrity rings especially true in the context of loan servicing, particularly for investors and loan servicers handling distressed loan portfolios. Often, *distressed paper* is connected with collateralized assets requiring bullet-proof substantiation in the event of court considerations and judgments. Having a system that can quickly find valid data supporting the rightful owners of such collateral can pay huge dividends.

With these factors in mind, we have developed eight critical steps loan servicers can take to ensure you and your investors are protected against security intrusions, data breaches and wieldy or inaccurate data.

**1) Don’t depend on spreadsheets**

It is almost always better to have a proven loan servicing software system in place versus a “system” of spreadsheet files and Word documents shared between disparate PCs, laptops and servers. These types of files can easily lose their integrity if links are broken or if formulas are erroneously changed by multiple users.

Disparate spreadsheets – or even unlinked, un-reconciled worksheets within the same Excel workbook file – present obvious issues. At best, weak data integrity creates an inefficient environment where reconciliations are forced by human intervention. At worst, bad or insufficient data can cost your business dearly when it comes to protecting collateral assets attached to the paper your organization either owns, or is servicing on behalf of another party.

There are a number of reputable loan servicing software platforms that can help alleviate both issues. A quick Internet search on “loan servicing software” yields a handful of software options.

---

2) **Find a software package with role-based security**

As you select a loan servicing software platform, it is important to consider a system with role-based privileges. Most loan servicing organizations have needs for production and business overhead roles such as loan originators, underwriters, asset managers / collectors, loan officers, servicers, customer support and accounting. Whether these roles exist inside or outside the company’s four walls has become irrelevant from an operating standpoint. It is imperative, however, that the common software system and database employed by the organization feature separate privilege levels, based on job responsibility. For instance, a collector may be able to update the comments section of an account but not the balance owed. As another segregation-of-duties policy, asset managers should be able to create portfolio results reports but may not necessarily be able to manipulate the data in those reports. Besides establishing accountability and better reliability, fewer people touching fewer areas of the system means the likelihood of foreign intrusions via malware is also mitigated.

3) **Implement field history reporting and solid audit trail capabilities**

Another key attribute of data integrity within a loan servicing package is the ability to establish an audit trail. You want to be able to quickly determine who made changes to an account and when those changes were made.

The software package you choose should have change fields within the account that cannot be deleted. Therefore, if changes are administered errantly, you can quickly pinpoint within your audit trail where the problem occurred and, of course, the responsible party. This level of accountability introduces a higher level of vigilance from your platform users and the ability to identify training needs.

A filtered query is a tool that can help your discovery process. A filtered query tool is important because it should be able to provide you with search results that are confined to a certain date range, a particular use or a set of users. It makes hunting for vital information quick and efficient.

An audit trail should be comprehensive, indicating when and where field changes were made, comments and documents were entered into the system, transactions were posted, or transactions were reversed.

The result of a smart choice in this area means you can expect an easier time with lenders and investors when audit time rolls around. Lenders and investors will have strong confidence in the integrity of the numbers and the value of their investment.

4) **Password protection**

Although it may be an obvious tip, it’s well worth re-emphasizing here. Distinct end user passwords that automatically expire within 60-90 days are a good way to ensure that only the right people are gaining access to your loan servicing system. Your policy should also prescribe a minimum password length, utilize a password history to ensure that passwords
aren't recycled, and a maximum number of log-in attempts before the system shuts out
the user completely. This process should be vigilantly managed too because individual
users tend to write down their passwords or place it among readily accessible
documentation on their individual PCs or laptops. Furthermore, a user's account should be
promptly deactivated upon termination.

A simple pathway to secure and reliable authentication is
the Single Sign-On (SSO) method whereby each user is
allowed to log on to all relevant systems without having to
log onto each of them independently, and have to
remember multiple passwords. Using Microsoft Active
Directory / Domain Authentication when signing into your
loan servicing software you are leveraging the domain as
your authenticating agent. This has the benefit of not requiring the user to remember
additional passwords, a consistent control on password strength and change frequencies,
and simpler administration. Besides the benefit of simplicity, security is greatly enhanced.

5) Protect against “data leakage” caused by internal resources

The proliferation of mobile endpoint devices such as laptops, cell phones, thumb drives,
and MP3 players has increased the threat of sensitive data “leaking” out of an
organization. A recent study by InsightExpress indicates that many technology users
disregard internal security policies and download unauthorized data and applications from
their work machines. In fact, more than half of the end users discussed in the survey have
changed the security settings on their business-issued notebook.9

According to Cisco, sponsor of the InsightExpress research:

“In the hands of uninformed, careless, or disgruntled employees, every device
that accesses the network or stores data is a potential risk to intellectual property
or sensitive customer data. Magnifying this problem is a disconnect between the
beliefs of IT professionals and the realities of the current security environment for
countless businesses. The new findings show that ‘insider threats’ have the
potential to cause greater financial losses than attacks that originate outside the
company.”40

Thus, implementing security policies on user devices is essential. If you don’t have
restrictions and policies on these endpoint devices, then you have a major hole in your
security plan. Placing Device Access Control Applications on individual computers in order
to restrict what runs in each PC’s memory is advisable. Additionally, placing policies on
USB drives is an ounce of prevention well worth the effort.

6) Use best-in-class security tools

You cannot have a meaningful enterprise data security conversation without talking about
anti-virus protection, firewalls, and layered intrusion detection systems (IDS). Enterprise-
class anti-virus and anti-spyware software should be installed not just on workstations, but also on file and mail servers. Most firewalls today have built-in anti-spyware and anti-virus capabilities but they do need to be activated in order for them to do their jobs. Always choose from reputable vendors.

Firewalls protect a network from outside hackers and other malicious attacks from the Internet. Through the use of firewalls, inbound Internet traffic can be monitored for any unauthorized web server attempting to access the organization’s network, to either download or upload data. An IDS monitors network traffic for suspicious activity and alerts the system or network administrator. Ideally, the IDS will respond to abnormal or malicious traffic by blocking the IP address.

7) Develop and implement a data backup and recovery plan

Many organizations today have unwarranted confidence in on-site data storage and backup processes. It is far too common to walk into a small- or mid-sized financial firm and discover either a tape or disk backup device. Equally alarming is that fact that the backed-up files are located in the same room, let alone the same building, as the production data. Besides natural disaster risks, events such as fires, hardware failures, power outages, hackers and disgruntled employees can also wreak havoc.

Many choose to back up with an on-site tape or disk system. But, because of the manual steps involved, tape backup is error-prone and resource-intensive. On-site disk storage systems hold a slight advantage over the tape process but also require off-site placement to ensure true recovery and business continuity.

Implementing an online backup and recovery process helps you avoid these problems. You can literally “set it and forget it.” Backed-up copies of data are immediately and securely moved offsite via an automated process that supports local and distributed enterprise sources. Loan data is compressed and encrypted on your local system and remains encrypted during transmission to a highly available datacenter. You decide how often data is to be backed up and how quickly you need it returned.

8) Outsource to a professional datacenter partner

“Play to your strengths,” the sports saying goes. These days, it just doesn’t pay to have all of your eggs in one basket, especially if that basket is an on-premise data closet stacked with servers and routers, a kludge of telephone and data wires, sans adequate power backup, cooling devices and technical support.

Furthermore, the most common point of attack on a corporate network is a personal computer or laptop. A user’s laptop can become infected through a remote Internet connection, and then infect the entire network. The points of vulnerability are dramatically reduced when your key users are all tapped into a system securely hosted on a managed server positioned in a protected and cool datacenter area.

Hosting your applications and databases off-site can be advantageous from a business
continuity perspective, especially for those smaller loan servicing organizations possessing significantly limited data security and backup resources, or those located in parts of the country where natural disasters may be a concern – such as coastal states with hurricane seasons or plains states prone to tornadoes or flooding.

Therefore, a strong datacenter partner may be a critical component of your data security plan. When searching for a partner, you should give special attention to those possessing SAS-70 Type II Audit credentials and advanced data protection facilities. The American Institute of Certified Public Accountants (AICPA) recognizes the SAS-70 Type II audit as a verification that adequate controls and safeguards are in place for service organizations possessing access to shareholder, client, and customer data.

According to leading datacenter experts, companies in the financial services industry have technical requirements for data hosting that make facility selection a very important decision. Datacenters need to be located in facilities with a combination of state-of-the-art features including advanced power, cooling and disaster recovery systems, redundant fiber connectivity, dedicated infrastructure, and superior physical security.

Today’s loan servicing world has been made more productive and efficient by information technology systems. But, as with other players in the financial services industry, loan servicers face challenges related to data security breaches, malware, bad data, leaked data and the growing need to report on data that may protect their financial interests.

By taking seriously the tips prescribed above, including:

- replacing spreadsheets with a proven software system;
- employing role-based security;
- implementing field history reporting and solid audit trail processes;
- employing authentication and password best practices;
- adequately protecting your endpoints from leakage;
- deploying best-in-class perimeter protection;
- introducing online backup; and
- partnering with a reputable provider of managed datacenter services...

...you will significantly decrease the likelihood that your loan operations will suffer the costly consequences of technology’s dark side.

About the author: Greg Hindson is president of the Nortridge Software, LLC. He can be reached via email at ghindson@nortridge.com or at his office phone at (714) 263-7251. Nortridge is a leading loan servicing software company headquartered in Lake Forest, California. The company possesses deep expertise in lending, banking, and software development. You may reach us at (800) 993-6227 or by emailing us at sales@nortridge.com. The Nortridge web site is: www.nortridge.com.