

SERVICING MANAGEMENT®

Reprinted with permission from the July 2006 issue

Stay Protected, But Be Sure To Not Bog Down Operations

Servicing companies need to ensure that customer information is safe, but should do so without causing operational inefficiencies.

There has been a lot of discussion recently related to security, mainly as a result of the recent data breaches and the growing importance of protecting consumer data. The discussions focus on the need and increased use of information technology (IT) systems, such as customized access-controlled systems, encrypted data technology and enhanced multi-factor authentication methods.



Gibbs

All these systems are put in place to ensure that consumer data is secure not only when borrowers access mortgage account information via the Internet, but also when servicing company employees access different systems and programs electronically.

While it is imperative to optimize the security of borrower's personal data, the reality is that the technology methods being implemented today are not enough to guarantee protection of data. The biggest risk to manage is still that caused by employees. Technology

Dawn Gibbs is president and chief executive officer of Financial Industry Computer Systems Inc. (FICS), a Dallas-based provider of mortgage loan origination, residential mortgage servicing and commercial mortgage servicing technology. She can be reached at dawn-gibbs@loanware.com.

BY DAWN GIBBS

systems can effectively be set to prevent intrusion, but when an employee does something that they should not - either unknowingly or maliciously - many IT security controls become irrelevant.

In today's environment, where security is required and increasingly important, financial institutions spend a great deal of time implementing systems and following government-mandated requirements to help protect consumer information. Consumer information that needs to be protected consists of any record containing nonpublic personal information, in paper or electronic format.

How much security?

How should mortgage servicers go about deciding what level of security protection is appropriate? To begin with, mortgage servicers should identify the reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information. They should also assess the sufficiency of the existing policies, procedures, systems and other arrangements already in place

to control risk and system integrity.

Since servicing companies need to reasonably ensure that their customer information systems (electronic or physical methods used to access, collect, store, transmit or protect customer information) are secure, they should aim to do so without causing inefficiency and excessive delays that could result in a less productive and profitable organization.

Mortgage servicers using outsourced service providers have yet another risk to consider. Disclosing information to an outsourced service provider increases the number of persons having access to the data, thereby creating additional risks to the security and confidentiality of the customer information.

In order to protect against these risks, an organization should implement appropriate steps to protect information that it provides to a service provider, regardless of who the service provider is or how the service provider obtains access. However, each servicer's methods for overseeing its service provider arrangements will not be the same for every provider. The risks posed by the provider should be considered, and then the correct method to protect the customer information can be put in place.

To address standards for developing and implementing administrative, technical and physical safeguards to



protect the security, confidentiality and integrity of customer information, there have been many regulations and guidelines enacted by the five member agencies of the Federal Financial Institutions Examination Council (FFIEC). These member agencies include the Office of the Comptroller of the Currency, Federal Reserve System, Federal Deposit Insurance Corporation, Office of Thrift Supervision and National Credit Union Association.

One such regulation that all financial institutions today are required to adhere to is the Gramm-Leach-Bliley Act. This act requires that financial institutions adhere to appropriate administrative, technical and physical safeguard standards to protect customer records and information. These safeguards are designed to ensure the security and confidentiality of customer records and information, protect against any anticipated threats or hazards to the security or integrity of records, and protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to any customer.

In addition, the Sarbanes-Oxley Act was passed in response to a number of major corporate and accounting scandals. These scandals resulted in a loss of public trust in accounting and reporting practices, which required that standards governing corporate responsibility, financial disclosure and information protection be implemented.

Mortgage servicers are utilizing various methods to help protect customer information. One way servicers are protecting information is implementing access controls on information systems. This includes controls to authenticate and permit access only to authorized individuals, as well as controls to prevent employees from providing customer information to unauthorized individuals. Restrictions permitting access only to authorized individuals at physical locations containing customer information - such as buildings, computer facilities and records storage facilities - is another securi-

ty initiative mortgage servicers are utilizing.

Robust authentication

A new, more robust form of security that mortgage servicers should consider for the future is the use of multi-factor authentication. This system ensures that a user is entitled to view data by implementing instruments such as fingerprint and iris scan devices. Combined with this system can be a graded authentication system - a security feature that requires users to input a sequence of authentication items (i.e., a fingerprint plus a password).

Access is given only to those users that log in using the assigned sequence, ensuring privacy and confidentiality. This also ensures the user is not able to copy or move files, which prevents secure information from being inadvertently moved to less secure areas. Multi-factor authentication may be necessary to increase network security beyond basic password authentication.

Even though the human factor is still the main source for security breaches, in today's electronic environment it is increasingly important to implement methods that will protect electronic information as well. When information is housed on a system that runs the risk of being unlawfully accessed remotely, it is subject to different types of risk and, therefore, requires a different type of protection than customer information stored as hard copies in a file drawer.

A method servicers are currently utilizing to protect electronic data is encrypting customer information, while in transit or in storage on networks or systems. Encryption, which alters the data so that it is unable to be read except by the intended recipient, requires use of a decryption key and program to decipher. An unwanted disclosure of certain information - such as account numbers or access codes - would be particularly harmful to customers. Therefore, the security measure implemented for electronic data needs to have an extra level of protection.

Many organizations have imple-

mented monitoring systems and procedures to detect actual and attempted intrusions into customer information systems. These organizations also have appropriate programs in place that specify actions to be taken when an organization detects that unauthorized individuals have gained access to customer information systems. This includes appropriate reports to regulatory and law enforcement agencies.

Background checks

One non-IT precautionary measure that mortgage servicers have implemented is background checks for employees with access to customer information. However, this process and the interpretation of the reported findings can be very subjective. Just because an employer performs a background check does not mean that the actual results were not questionable or open to individual interpretation. Where is the line when employers say the person is not trustworthy enough to hire? Is someone who was caught shoplifting a 10-dollar item 20 years ago considered to be too untrustworthy to deal with customers' personal information today?

One recent survey commissioned by the Computing Technology Industry Association Inc. reported that human error was responsible for 60% of respondents' security breaches in 2005, while only 20% was due to technical malfunctions. Written IT policies, which include procedures for disabling former-employee access, and continual security awareness training are two areas that are credited as reducing breaches. It is further important to limit access to information that discloses vulnerabilities. Another report identified that more than 50% of attacks were performed by persons who exploited known vulnerabilities in systems and procedures.

Mortgage servicers must design their information security program to control the identified and reasonably foreseeable risks and threats in a timely and cost-efficient manner. Requiring all organizations to have the same degree of protection for customer information may be unnecessarily burdensome in many cases, especially if

the cost, maintenance and restrictiveness of the protection are more than what is justified by the risk. Furthermore, protection of customer information increases a servicer's operational costs - a cost which, at some level, is passed through to the consumer.

Thieves

While having technology security processes and procedures in place is a necessity and a requirement, there is always going to be some sort of

risk when it comes to customer information - especially since the human factor continues to exist. Even the most trusted of employees can perform acts of thievery. The most physically secure companies can have their walls permeated. And the most well-respected firewalls can't protect against the unknown, ruthless hacker.

The security program that servicers implement should include measures to protect against reasonably foreseeable risks - both electronic and actual hu-

man threats. In today's environment, some level of risk will always be a possibility. It is important to have technological security in place, but also a healthy balance among technology tools, protection against the old-fashioned human factor and some common sense.

The best advice is to keep your eyes and ears open, continually review your procedures and security controls, and be ready to act quickly in the event of an intrusion or unauthorized disclosure. **SM**