Security

Sorry, We Can't Close Loans Today

The importance of securing your loan origination system - and everything integrated with it.

By Jim Deitch & Allen Harper

A CEO recently took a call from his secondary market manager: "Why can't we close loans today? Why can't I get the hedging data?" Great questions, but no answers - at least for a couple days.

The single point of failure for mortgage banking and related activities can be the loan origination system, or LOS. Integration of ancillary systems into the LOS improves efficiency but can also create vulnerabilities that, in turn, may affect uptime. As a result of such failures, the mortgage banker can suffer reputational and financial damage. Worse, customers might not be able to close loans, and Realtors might see multiple deals delayed. Worse still, such outages might catch the attention of regulators who may end up subjecting the mortgage banker to yet another "targeted exam" concerning operational risk. How can a mortgage banker prevent this situation?

The LOS is a "critical system" for a mortgage banker. This is both a practical description, as well as a term of art. Practically every employee in the origination process, from originator to shipper, uses the LOS or data from it. A "critical system" in regulator parlance means the system can be a key source of operational, financial, compliance, information security and reputational risk.

Failure of critical systems is not as remote as one might think. Hurricane Sandy brought at least one major supplier of bank "core loan and deposit systems" a multiple-day outage of core systems for its bank clients. This was the culprit: Flooding in a core system provider's data center caused a

cascading series of operational problems that affected other data centers and knocked multiple banks "out of business" for several days. In some cases, the banks were hundreds of miles inland from New York City.

The LOS is also a critical system for information security. The "safeguards" rule of the Gramm-Leach-Bliley Act (GLBA) calls for lenders to utilize the best security approach that is both readily available and cost effective. LOSs are prime targets for breach of customer data - both mortgage banking data, as well as other systems on a mortgage banker's network.

How does a lender manage critical systems to reduce the possibility of a system failure? A lender should perform a detailed risk assessment of its LOS and related systems that covers at least the following:

- How effective is the lender's disaster recovery plan or business interruption plan for mortgage banking? Has the plan been tested to assess its effectiveness?
- What ancillary systems (hedging, pricing engine, loan delivery, post-closing, servicing) may be affected by an LOS failure?
- Has the lender's LOS been tested for information security, both traditionally and by "ethical hackers?"
- Does the lender have backup systems to perform essential functions in the event of a critical system failure? Is there a series of step-up actions triggered if a failure persists beyond an hour? A day? Two days? What if the system fails at month-end? Quarter-end? At mortgage-backed securities (MBS) settlement days? Do the backup systems actually work? How long will the backup systems remain effective in the event of an extended outage?

Risk assessment

A risk assessment examines the

end-to-end business model, systems, procedures and business continuity plans of a lender. It also assesses information security - but more on that later. Mortgage banking usually has business model risks that other financial services do not have: loan officers in branch offices, in the field, at Realtors' offices or at other public locations. The ability to disclose accurately, meet tolerances for estimated costs, close as planned and deal with changed circumstances within regulatory time periods puts additional compliance pressures on lenders.

The interdependency of systems should be assessed. Pricing engines, disclosure modules, hedging systems, document preparation, compliance testing and credit reporting may come from discrete vendors, but if services are delivered to or accessed from an integrated LOS, users can experience widespread unavailability of related systems. A business continuity plan should assess the possibility of a single point of failure from an integrated LOS affecting independent related systems. Long delays could ensue as the lender "unbundles" access.

Some lenders, on the other hand, have considered the single point of access as a failure mode and have standby access methods. Others have standby access, as well as a backup document supplier independent of the bundled supplier. These lenders experience inconvenience during a widespread, two-day LOS failure event; however, the lender is able to close loans despite the failure on the last day of the month - to the delight of clients, Realtors and builders.

Effective risk management requires that a lender plan for a loss of the critical vendor services when building a business continuity plan. Assessment of the possibility of vendor failure can be done through effective "critical vendor" management.

Finally, an information security assessment should be conducted from both the lender's viewpoint and from that of a malefactor intending to penetrate the system. The assessment should include effective implementation of traditional security controls (firewalls, system controls, etc.), as well as an assessment of cultural controls: How well do employees actually comply with information security policies and procedures?

Critical vendor management

A "critical vendor" requires careful management. Part of the risk assessment should cover assessment of the vendor's independent Statements on Standards for Attestation Engagements (SSAE) 16 "Service Organization Controls" report. The Service Organization Controls (SOC-1) independent report is issued after an independent audit of the vendor's system, system controls, backup systems and effectiveness of the controls. The SOC report generally consists of the following:

- Whether the controls were suitably designed and operating to provide reasonable assurance that the control objectives are achieved: About a dozen or more control objectives are identified. Typical control objectives may be "control

activities providing reasonable assurance that physical access to vendor data centers, system and network equipment, and storage media is limited to authorized individuals," or activities that "provide reasonable assurance that vendor facilities housing customer equipment and support operations are designed and monitored to reduce the risk of environmental threats (e.g., power loss, fire, flooding)."
- Identification of complementary user entity controls that is a non-comprehensive list of the controls that customers are responsible for having in place for all control objectives stated by the SOC report to operate effectively: Pay particular attention to the organization's use of complementary user entity controls. If any of these controls are missing or ineffective: the vendor's reliance on the complementary controls means its control objective may not be achieved.
- The controls and testing of operating effectiveness results summary lists exceptions noted in testing: Pay particular attention to exceptions noted, and if not reported, query the vendor to determine if the exceptions have been remediated.
- Conclusion and recommendations should conclude that the vendor's systems, network and hosting services are adequately secure, provide processing integrity and availability as contracted, and provide confidentiality of the lender's data.

It is absolutely critical that the lender ensure the complementary user entity controls are in place and are effective at every lender location. It is also critical to provide appropriate backup and work-arounds for any failures that may occur with the critical vendor.

Finally, determine if the vendor has any enforcement agreements issued by regulators against it. One can determine the presence of such enforcement orders by visiting the Office of the Comptroller of the Currency or Federal Deposit Insurance Corp. websites. If an enforcement order exists, ensure the lender has additional controls in place to compensate for vendor shortfalls until the vendor corrects them.

LOS security

LOS security is critical. What follows are examples of security issues affecting customer information security and personal identifiable information (PII) breaches that actually occurred. Importantly, almost all of these lenders had penetration testing, information technology audits and other IT testing performed, resulting in a false sense of security:

- Example 1: Through a combination of weak levels of user security awareness training and poor laptop configuration, a bank employee with a laptop inserted a malicious USB thumb-drive file, causing complete laptop compromise, which a hacker used to obtain complete network compromise, including LOS application, customer data breach, and a gateway into other bank systems in a federally insured bank. This breach may have resulted in the Real Estate Settlement Procedures

Act (RESPA), GLBA, Bank Secrecy/Anti-Money Laundering Act and other regulatory violations.

- Example 2: A mortgage branch manager was granted administrative super-user access as a substitute for a properly configured LOS persona. Loan officers of record were changed, permitting unregistered loan officers access to the system, some of whom were not current employees. Under-the-table cash payments for commissions, national multiple listing service exceptions and complete breach of the bank's Information Security policy occurred in a federally insured bank. This breach may have resulted in RESPA, the Secure and Fair Enforcement for Mortgage Licensing (SAFE) Act, GLBA and other regulatory violations.
- Example 3: An employee with a laptop with an LOS installed clicked on a "spoofed" Wi-Fi connection that was thought to be secure. Login information was stolen, and systems were compromised through insertion of malware by an unauthorized user using the stolen credentials. Additional compromises resulted from insertion of keystroke logger and other malware, leading to lateral movement to other bank systems. This breach may have resulted in RESPA, GLBA and other regulatory violations.
- Example 4: Poor controls over a lender's loan pipeline of leads and loans in process resulted in duplication of this information by a branch manager and loan officers, which moved this data to a competitor upon its resignation from the lender. This resulted in economic losses to the lender, as well as likely SAFE Act, RESPA, GLBA and other regulatory violations.
- Example 5: Weak system controls allowed loan closing packages to be redirected to a "ghost office." Loans were likely brokered away from a lender, and closing packages were potentially altered at the ghost office. These issues resulted in violation of the lender's correspondent agreements, and, likely, SAFE Act, RESPA, GLBA, and U.S. Department of Housing and Urban Development as well.
- Example 6: Loan underwriting data was changed by an origination employee working in concert with another employee with inappropriate administrative access; loans were closed that did not conform to underwriting guidelines due to alteration of underwriting transmittal. The result was unsalable loans that the lender had to dispose of at a loss, as well as likely RESPA and SAFE Act violations.

These incidents resulted in material, financial, operational, compliance and reputational risks to the lender, and a compromise of the systems. Two of the above cases were performed by us, using ethical hacking to assess and test the actual level of security in effect for the client. In both ethical hacking cases, access to bank wire transfer systems was achieved, including access to telephonic passwords to confirm wire transfers.

Fighting back

A comprehensive security program should be established to measure, monitor and reduce security threats. It is not a one-time event. Effective security is a continual process of staying one step ahead of a security breach. Following are best practices in such a security program:

- Security risk management assessment: Conduct a risk assessment and gap assessment from an attacker's point of view to determine the current security posture and risk profile. Consider the types of physical, cultural, operational, system and internal control breaches that innovative hackers and employees could perpetrate. Develop a security road map and implement security best practices to improve the organization's security maturity level. It's vitally important to assess and test physical, cultural and technology controls in tandem.
- Use a secure document management system: Traditional fax and email should be replaced and integrated with secure document management services with built-in document fax, scanning, encrypted email, document management, version control and delivery to the actual LOS.
- Apply best practices for physical security: Ensure that appropriate levels of physical security are in place to limit access to the sensitive data storage, data centers, network infrastructure and host systems. Top-tier data centers require multiple levels of physical security, including monitored cameras, security alarms, biometric authentication mechanisms, electromagnetic locks with logging capability, identification badges, and formal policies and procedures for controlling access.
- Apply best practices for network security: Firewalls, enterprise-class routing and switching equipment should be configured with appropriate security features such as access control lists and virtual local area networks for sensitive network segments. Network servers and hosts should be configured in a patched and hardened manner. There should be proactive detection and monitoring of network anomalies and intrusions. A security information and event management device should be installed and tuned properly to detect attacks and worm breakouts in real time. A formal incident-response plan should be developed and exercised on a regular basis.
- Apply best practices for application security: The LOS should be configured using best practices to secure the sensitive client and loan data from start to finish. Assess the ease of use versus security trade-offs. Oftentimes, the careful deployment of user persona with information access controls can provide ease of use and appropriate levels of security. The LOS should provide sufficient levels of password authentication, encryption and access controls to comply with the company's security policy. The

application should allow for the establishment of roles, rights and access views for defined parties. A detailed audit log should be provided that shows all access (by username and time stamp) to information and system configuration changes. The application should provide for the exchange of information to all parties within the application and not require the unsafe copy of information outside the system.

- Train employees: The root causes of all the security incidents referenced earlier were employees failing to follow established company practices. All employees, particularly those in the field, need periodic training regarding safe computing practices. Frequent auditing of users with administrative rights is imperative. Instruction on social hacking methods is a must, as many employees do not fully appreciate the damage caused by "decoy" USB drives, social engineering, spoofing or email/Web-delivered malware.
- Assess and test: Effective security requires careful and frequent risk assessment followed by well-designed testing. The information security breaches described above occurred in banks and mortgage banks that believed effective security measures were in place. Testing should incorporate physical, logical, internal control and social control testing. Virtually all of the system compromises described above were not brute-force attacks on a system or network; rather, they occurred by employees circumventing established controls or hackers who exploited common weaknesses in the overall system of controls.

Through a combination of risk assessment, remediation, vendor management and appropriate business continuity planning, LOS and related system risks can be effectively managed.

Jim Deitch is CEO and co-founder of Teraverde Management Advisors, a provider of mortgage banking, loan origination system, compliance and capital markets expertise to banking and mortgage banking clients throughout the U.S. He can be reached at jdeitch@teraverde.com. Allen Harper is executive vice president and "chief hacker" at Tangible Security Inc., a partner of Teraverde. He can be reached at aharper@tangiblesecurity.com.