TERAVERDE®

TANGIBLE SECURITY
A CYBERSTEP AHEAD

Loan Origination System Security - “A Reporter is on Line 2”

A CEO client recently took a call from national news reporter: “Why did the lender report losses from mortgage operations?” Of course, he couldn’t publicly answer the questions. Poor security led to a variety of financial losses. The bad press caused further reputational and financial damage. We authored this white paper to assist bankers and mortgage bankers to avoid the root causes of security breaches, the financial and reputational damage, and of course the dreaded calls from reporters.

Purpose

This white paper briefing outlines the security risks involved with Loan Origination Systems, and handling loan applications and documents, and describes industry best practices for the protection of lending documentation and personally identifiable information (PII).

Problem

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. Companies deploy technologies and compliance efforts, but never really get an assessment of “ground truth”, from an attacker’s point of view. A recent survey showed that 70% of lenders expose sensitive client and loan data through emails [1]. Next to emails, fax machines may prove to be the weakest link and a significant security risk to lending organizations. Fax machines are not the best practice for secure document delivery and may be vulnerable if not locked in a secure access location with restricted access to those with a need to know [2].

Lenders are under pressure to produce more, at lower costs. This pressure is causing some lenders to compromise between security and speed. Some lenders have misconfigured the Loan Origination System (LOS) and have unknowingly put themselves and their client’s data at risk. Other lenders may have a properly configured LOS, but a poor level of security awareness among users may undermine the effectiveness of the controls. Finally, sometimes “good people do bad things” and circumvent the established security policies and protections in place [3]. Attackers are beginning to target the loan origination systems; recently two Hackers were caught after causing more than $100,000 of losses to customers [4]. A comprehensive security program should be established to measure, monitor, and reduce security threats. It’s not a one-time event. Security is a constant process of staying one step ahead of a security breach. The best practices section of this document is a good start to establishing such a security program.

Examples of Recent Findings

- Through a combination of weak levels of user security awareness training and poor laptop configuration, a bank employee with a laptop inserted an infected 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.
- Weak internal security controls at a lender left systems vulnerable to attack and lateral movement across the network. Several systems were compromised including LOS, CRM and bank file server applications were accessed by attacker.
- A mortgage branch manager was granted administrative ‘superuser’ 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 which were not current employees. Under the table cash payments for commissions, NMLS exceptions, and complete breach of the bank’s Information Security policy occurred in a federally insured bank.
- A bank screened mortgage loan officers, but the traditional screening methods did not detect that two different loan officers were under federal indictment for mortgage and financial fraud from prior employment. These employees continued to work at a mortgage branch office and had access to LOS systems, credit reporting, financial records of customers at a federally insured bank.
- Loan Origination System access was granted to users without clearance from HR and prior to execution of employment related documentation (including NMLS registration and licensing). Unlicensed/unregistered loan officers originated loans and had operational access to systems.
- Improper LOS configuration permitted ‘loan originator of record’ fields to be edited by the branch; normally this data is secured and can be changed only by central supervision. This allowed registered NMLS employee to appear as originator of record, but the originator of record field was changed at a later time so that another employee could be paid commission.
- An employee clicked on a ‘spoofed’ Wi-Fi connection that was thought to be secure. Logon information was stolen, and systems were compromised through insertion of malware into the initial compromised laptop. Additional compromises resulted from insertion of keystroke logger and other malware, leading to lateral movement to other bank systems.

- 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. They moved this data to competitor upon their resignation from the lender.
- 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'.
- Loan underwriting data was changed by an operational 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.
- Government Monitoring Data was altered after loan closing by an individual that did not originate the loan, resulting in inaccurate GMI data.
- Loan pipeline data was transferred to USB drive without authorization.
- Each of these incidents resulted in material risk to the lender, and compromise of their systems. More importantly, almost all of these lenders had penetration testing, information technology audits and other testing performed, resulting in a false sense of security. Several of the above cases were compromised using ethical hacking by our team to assess and test the actual level of security. In two ethical hacking cases, access to bank wire transfer systems was achieved, including access to telephonic passwords to confirm wire transfers.

Best Practices

- 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 roadmap 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 with integrated secure document management services with built in document fax, scanning, encrypted email, document management, version control, and delivery to actual Loan Origination Systems.
- 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. Outsourced, multitenant data centers should provide a valid certificate of SAS 70 Type II inspection [5].
- Apply Best Practices for Network Security. Firewalls, enterprise class routing and switching equipment should be configured with appropriate security features such as access control list and VLANs 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 (SIEM) 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 in a best practice manner 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 meet the company 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 timestamp) 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.
- 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 bankers 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, the breaches occurred by employees circumventing established controls, or hackers that exploited common weaknesses in the overall system of controls.

About the Authors

Jim Deitch CPA, CMB is co-founder and Chief Executive Officer of Teraverde Management Advisors, and was co-founder of three national banks. Teraverde provides mortgage banking, LOS, compliance and capital markets expertise to bank and mortgage banking clients throughout the US.

Allen Harper is the Executive Vice President and "Chief Hacker" at Tangible Security, Inc. (a partner of Teraverde). Mr. Harper is a recognized author, speaker and teacher. Notable, he is the lead author of Gray Hat Hacking, the ethical hackers' handbook, now in its 3rd edition. Tangible Security provides a wide range of cyber security services to commercial and government clients.

References

[1] PR Newswire, "Halock investigation finds that over 70% of mortgage lenders may be putting sensitive financial data through their application processes," PR Newswire US, Jan. 2014.

[2] P. Huff, "Could fax be the weak link in your security chain?," Mortgage Banking, vol. 67, no. 5, p. 101, Feb. 2007.

[3] J. Blythe, R. Koppel, and S. W. Smith, "Circumvention of security: Good users do bad things–," IEEE Security Privacy, vol. 11, no. 5, pp. 80–83, Sep. 2013.

[4] Courthouse News Service, "Mortgage Hackers Accused of Stealing $100,000," 03-Mar-2014. [Online]. Available: http://www.courthousenews.com/2014/03/03/65767.htm.

[5] J. Phillips, "Securing mortgage documents in an online world-from origination to funding," Mortgage Banking, vol. 66, no. 9, pp. 121–122, Jun. 2006.