NATIONAL MORTGAGE PROFESSIONAL MAGAZINE
nmp
The source for top originators

Managing Two Key Operational Risks for Mortgage Lenders

By Jim Deitch

In the past several years, mortgage lenders have focused on the development and implementation of risk management policies, procedures, programs and practices. Yet, regulators seem to cite two areas where operational risks still constitute frequent regulator critique.

- **Lender Secrecy/Anti-Money Laundering (BSA/AML):** BSA/AML is a regulatory risk that requires careful and extensive planning and governance by every lender. Executives should ask what types of customer AML risk is my lender willing to take? Has the lender's risk management function managed these risks sufficiently to mitigate the risks the lender is willing to accept? Have the lender's systems and BSA/AML automated tools been integrated and calibrated to detect and manage the specific types of customer risk the lender's business plan accepts?

  Has the lender validated and tested the BSA/AML automated tool calibration and effectiveness vis-a-vis the lender's consumer and business customer profiles? Oftentimes, lender executives are criticized over lack of initial and periodic validation of the BSA/AML monitoring tools and clearance of exceptions. Thoughtful consideration of the specific risks that a lender undertakes with its customer base, and effective monitoring of these risks, can avoid regulatory criticism and enforcement action in the BSA/AML areas. BSA/AML automated tools must be calibrated to specific customer threshold limits to be effective. Periodic testing and validation of these limits and system effectiveness should be considered in view of "false positives" and "false negatives."

  Self-initiated model review and back testing of BSA/AML monitoring tools can go a long way in effective governance and avoidance of exam findings and enforcement actions, according to a managing partner at a national law firm that assists lenders with enforcement actions in BSA/AML. Ineffective AML monitoring can lead to enforcement action, civil money penalties or worse.

- **IT and Cybersecurity:** Another area of operational risk is cybersecurity, cyber-attacks, customer data breaches, and resulting damage to one's reputation and financial losses. Don't think a "clean" penetration test means you are not at risk. Lender senior executives make three common mistakes regarding cybersecurity: The senior executive lets the IT manager handle cybersecurity testing; the executive team does not view IT security in global terms that include employee and vendor compliance with IT security policies; and the senior executive does not demand a comprehensive and frequently tested Security Incident Response policy to guide their lender's reaction to possible security incidents.

  Another common mistake is to have the wrong kind of cyber insurance. Companies find out that coverage can be denied because security procedures listed on the insurance application were not meticulously followed or were ineffective. Some policies do not cover the loss of revenue arising from a breach, or do not fully cover remediation costs.

  Lender executives should remove responsibility for cybersecurity testing from the chief information officer. Independent testing is a

NMP MEDIA CORP.
1220 Wantagh Avenue • Wantagh, New York 11793-2202
516-409-5555 • Fax: 516-409-4600 • E-mail: advertise@NMPMediaCorp.com
NationalMortgageProfessional.com

fundamental security control, and cyber testing should be rotated among third-party firms periodically. IT security testing should emulate realistic threats and should not be confined to simply probing the firewall. Most mortgage bankers have laptops in the field and at production offices. Loan officers can also be sources of vulnerability, as they often receive information from customers via e-mail. Poor security can introduce malware into the lender's systems.

Effective cybersecurity assumes that a non-authorized user will gain access. Effective risk management of cybersecurity includes IT security controls that prohibit thumb drive and other device installation on lender computers. It includes employee security policies that highlight the threats of clicking on phishing e-mails, verifying the security of WiFi networks and frequent training and testing of human frailty exploits: Phishing, poor physical control of lender premises and careful and continuous vendor management. It includes designing and testing the segregation of system access and segregation of data to limit damage if an unauthorized intruder gains access to a lender network or system. The arc of risk in cybersecurity encompasses all lender employees, trusted vendors and all of the elements of the lender's IT systems.

Effective risk management assumes that lender IT systems will be penetrated. A cybersecurity program must address how will penetration be detected, what is the security incident response, and how can the lender's IT systems be designed to minimize movement laterally across lender systems in the event of penetration. Finally, effective risk management assumes that the lender has already been penetrated and an Advanced Persistent Threat (APT) is lurking somewhere within the IT infrastructure. APTs include malware that lies dormant, awaiting the command to open a back door, or malware that slowly, but unobtrusively, infiltrates valuable and confidential customer data over time.

While these two operation risks may seem very different, they both are high profile regulatory initiatives and both have "headline risk" and enforcement risk that senior executives should manage.

James M. Deitch is chief executive officer and co-founder of Teraverde. He has successfully implemented residential lending strategies in his banks, and served on the Mortgage Bankers Association Board of Governors for three terms representing a community bank lender in the MBA. He may be reached by phone at (855) 374-TVMA.