Mortgage Industry Faces Cybersecurity Challenge

Expanding online business creates more opportunity for malicious hacks

By Paul Lewis and Jeff Bernstein

The migration to cloud platforms, along with the adoption of self-service Web portals and mobile-device applications, has changed the nature of most traditional financial-service computing networks. The entire sector continues to be placed under pressure from malicious users and well-crafted cyber-attacks.

These increasingly pervasive attacks place organizations under ongoing pressure to protect mission-critical applications and connected electronic infrastructures. Although attacks in the past were network-centric and aimed at disabling the infrastructure, attackers now are aiming their sights on end-users, their credentials, the applications that they access and the sensitive private data stored within them.

Arguably, mortgage originators collect more personal data from their customers than most other players in the financial services sector. This makes them a desirable target for cyberattackers. Typical home-loan applications require mortgage originators to acquire the following from borrowers:

- **Tax returns and W-2 forms**
- **Driver licenses and other IDs**
- **Pay stubs**
- **Confidential credit-report information**
- **Recent bills**
- **Banking statements**

There also is the matter of ensuring secure data transmission, as typical mortgage transactions involve the sharing of private data between multiple parties, including the borrower, the lender, servicers, insurers and attorneys. The need to be competitive drives companies in the mortgage industry to place emphasis on ease-of-use and ease-of-access. Unfortunately, ease-of-use and accessibility often come at the expense of security.

Data-security compromises ultimately create very costly and difficult situations for organizations to recover from and can lead to many problems, such as: identity theft; loss and leakage of private date and sensitive information; fraud; theft of funds; theft of intellectual property; sabotage; disruption of business; and damage to brand and reputation.

Securing digital assets

A recent report by the law firm Foley & Lardner LLP suggests that mortgage originators in particular need to better secure their digital assets and should prepare for increasing, targeted cyberattacks.

The report revealed the following:

- **Three years ago,** there were about 93 million records lost in data breaches worldwide;
- **Two years ago,** the number of lost records increased to 552 million;
- **This past year,** the number of records lost because of targeted attacks increased to more than 1 billion.

Although the mortgage industry has historically avoided Target- and Sony-sized data-breach catastrophes, the days of operating off the radar of cyberattackers are likely coming to an end. Recent high-profile cybersecurity compromises should serve as a dire warning to the entire mortgage-lending sector.

More regulations

In December 2014, the New York State Department of Financial Services (DFS) issued an industry guidance letter to banks outlining the specific issues and factors on which those institutions will be examined as part of new targeted, DFS cybersecurity preparedness assessments. The banks will be examined on their protocols for the detection

Continued >>

Paul Lewis is vice president of technology risk at T&M Protection resources. A 20-year veteran of the security services industry, Lewis has spent much of his career providing counsel to financial-service companies on data forensics and information security matters. Reach him at plewis@tmprotection.com.

Jeff Bernstein is managing director of the information security advisory group at T&M Protection Resources. He has more than 16 years of experience leading organizations dedicated to protecting critical electronic computing infrastructure. Reach Bernstein at jbernstein@tmprotection.com.

Scotsman Guide

Reprinted from *Scotsman Guide* Residential Edition and **ScotsmanGuide.com**, August 2015

<< Continued

of cyber breaches and penetration testing, corporate governance related to cybersecurity, their defenses against breaches, the security of their third-party vendors and a number of other factors.

The new cybersecurity assessments will become regular, ongoing parts of all DFS bank examinations moving forward. Similar initiatives have and/or will be implemented by other financial services authorities, including but not limited to the Federal Deposit Insurance Corp., the Office of Thrift Supervision and the Federal Financial Institutions Examination Council.

Regulatory mandates, including the Sarbanes-Oxley and Gramm-Leach-Bliley acts, as well as direction provided by the National Institute of Standards in Technology (NIST), also place significant emphasis on securing networks and the confidential data that reside within them. Given the rising profile of the security exposures faced by the mortgage industry, increased regulation should be expected.

Mitigating the threat

A cyber-preparedness program will typically begin with the identification, classification and prioritization of the organization's information assets. This process forms the basis for a threat model.

Once prioritization of all computing infrastructure is complete, a risk assessment should be delivered to baseline the security posture of the corporate network. The risk assessment should typically consider the probability of attack as well as the potential impact to business if a successful attack was to occur.

The probability component should consider security threats, vulnerabilities and other deficiencies. The impact component is usually measured in terms of cost. The combination of these values should be considered the total risk involved.

Based on the risk-assessment findings, the organization then develops a well-tailored risk-management plan. This plan proposes countermeasures for addressing risk that involve eliminating, mitigating, accepting or transferring (to third parties). The plan takes into consideration prevention, detection and response components.

A commonly accepted information security framework — like the NIST's Framework for Improving Critical Infrastructure Cyber-security, which incorporates ISO 27K — also may be utilized during the implementation of the information-security management plan.

Countermeasures may include the implementation of technology, the development and implementation of policies and procedures, and the education of staff.

The cost and benefit of each countermeasure should always be considered by the organization, which should not seek to eliminate all risks but simply to manage them in the most reasonable and cost-effective way.

After the risk-management plan is implemented, it is tested and evaluated with regularity and preferably by means of formal third-party security assessments. Security managed in this fashion becomes an enabler to the success of a mortgage company. ■