# Navigating Hacker-Infested Waters

## Don't get pulled under by mortgage security breaches

By James M. Deitch

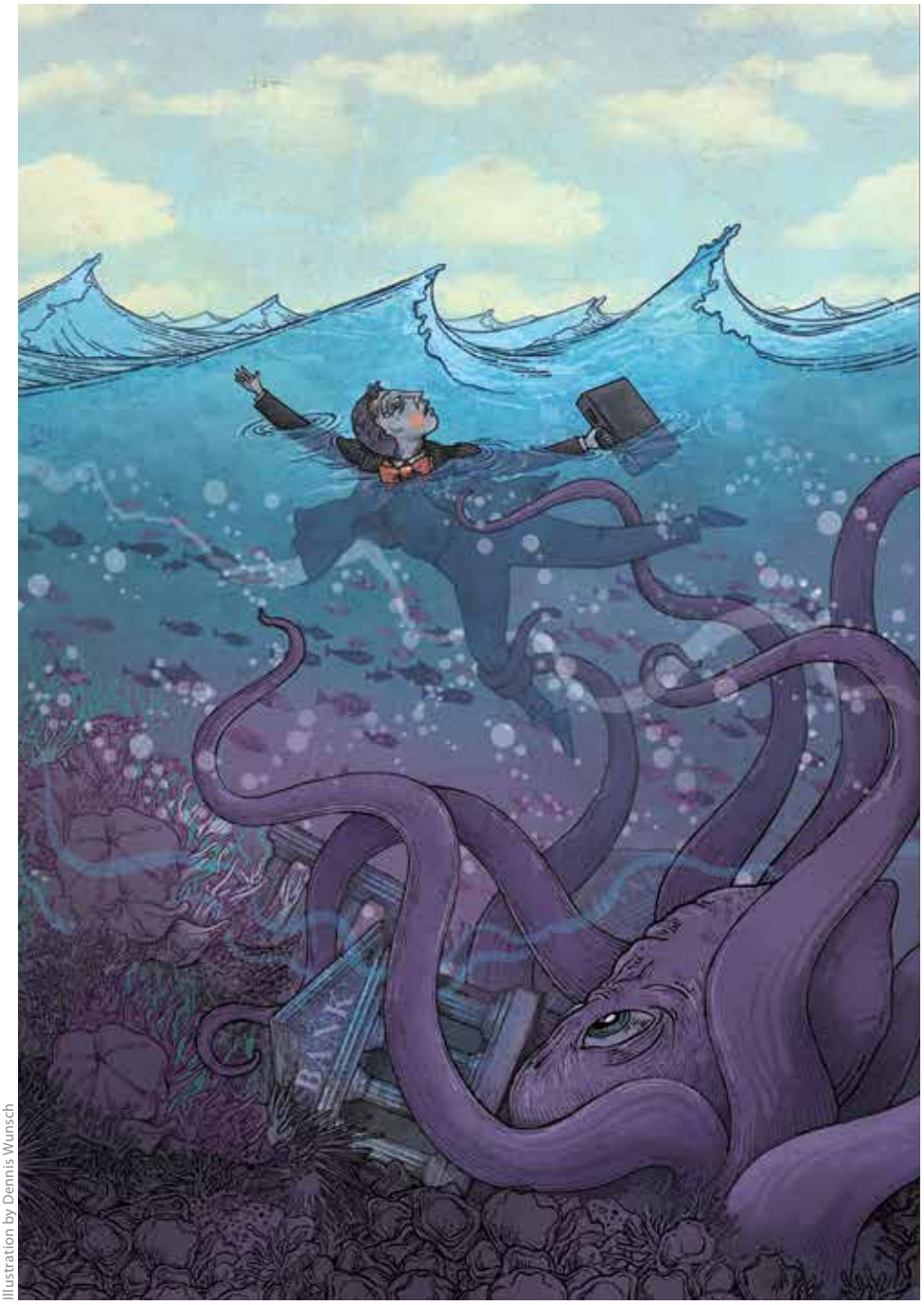

Illustration by Dennis Wunsch

When the executive vice president (EVP) of loan production picked up the phone, an excited voice on the other end yelled, "Someone stole our pipeline!" Astonished, the EVP asked for clarification, to which the caller replied, "Our active pipeline and closed loan database were stolen." The EVP's normally optimistic mood hit the floor. Worse yet, the EVP realized that the Consumer Financial Protection Bureau (CFPB) was due in the office in two weeks. Sadly, this scenario didn't have to happen this way.

Historically, information security was the purview of the information technology (IT) department. Information security is no longer just about firewalls and technical systems, however. It is a business strategy that must be embedded throughout mortgage-banking operations. With security breaches growing at alarming rates, it is clear that information security must be a key priority for CEOs and chief production officers if they want to keep their companies afloat.

Continued >>

**James M. Deitch** is co-founder and CEO of Teraverde Management Advisors, and was founder of three national mortgage banks. Teraverde provides mortgage banking, loan origination systems (LOS) and information security services, including "ethical hacking assessments" to bank and mortgage banking clients throughout the U.S. Reach Deitch at jdeitch@teraverde.com or (717) 327-4083. Visit www.teraverde.com.

Scotsman Guide

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

<< Continued

The Mortgage bankers deploy branches and loan officers to remote locations. The loan origination system (LOS) used in all of these locations is a treasure trove of personally identifiable information (PII), including credit reports, social security numbers, employment histories and lists of assets — everything a criminal could want. It also contains information that ethically impaired loan officers or branch managers might want to remove from the premises should they decide to jump ship.

If you think your systems are secure enough, you haven't been paying attention to the news over the past few years. Consider the following tales from the trenches of mortgage banking, which illustrate the many easy ways your security can be breached.

## Bypassing anti-virus software

A bank employee inserted a virus-infected USB thumb drive into a laptop, compromising the laptop. The virus contained a keystroke logger and other malware a hacker planned to use to compromise the bank's entire network, including accessing the LOS application and customer data files. The hacker leveraged the employee's laptop as a gateway into other bank systems in a federally insured bank.

You may think, "This can't happen to us. We use anti-virus software." Anti-virus software recognizes signatures of known threats. Hackers simply write code that hasn't been widely distributed, insert it on a USB thumb drive and bypass anti-virus detection.

## Misusing access privilages

A mortgage branch manager was granted administrative "super user" access as a substitute for properly configured, level-appropriate access. The manager used this access to give unregistered loan officers, some of whom were not current employees, access to the system. This issue blossomed into under-the-table cash payments for commissions, National Mortgage Licensing System (NMLS) exceptions and a complete breach of the lender's loan origination system. The branch left the company in a group walkover to another lender, taking mortgage leads, pipeline data and personal client information with it.

Many LOS systems are provided as software as a service, meaning an external provider hosts the system and provides overall system security. The lender's system administrator should maintain access controls, but excessive system privileges are often permitted because of poorly defined LOS roles and responsibilities. Excessive user privileges are often at the heart of data losses.

Inadequate controls of a lender's leads and loans in process resulted in this information being duplicated by a branch manager and loan officers. They moved this data to a competitor upon resignation.

In another case, a lender belatedly found that a recently hired top loan officer had transferred the entire contents of a former employer's laptop — several gigabytes of information — to the new lender. Of course, this included PII and other proprietary information belonging to the former lender. This situation was a lawsuit waiting to happen.

Information security does not only involve technical systems. You must also pay attention to the procedures used to monitor access to your origination system and your data. Make sure these procedures can track what is being removed and by whom, as well as what is being imported and by whom.

## External-access risks

A loan officer clicked on a "spoofed" Wi-Fi connection while sitting in a nationally known coffee shop. The spoofed network had a familiar name from the coffee shop. Through this false connection, a hacker obtained control of the loan officer's e-mail and proceeded to steal lender and client information over an extended period of time.

Today's electronic mobility opens up lenders to breaches wherever employees do business. Even if your internal network is secure and your IT personnel monitor access closely, your data is still at risk if employees do not take care to stay secure outside the company's walls.

## Lessons learned

These incidents resulted in material risk to the lenders and a compromise of their systems. More importantly, almost all of these lenders had performed penetration testing and rudimentary information technology audits, which resulted in a false sense of security.

Some lenders have misconfigured their loan origination systems, unknowingly putting themselves and their client data at risk. Other lenders have properly configured the LOS, but poor user security awareness undermined the effectiveness of these controls. Sometimes, good people do bad things and accidentally or unwittingly circumvent established security policies and protections, while some "bad apple" employees may even intentionally circumvent controls.

What is a CEO or chief production officer to do? Following are best-practice recommendations for security enhancement:

- **Risk-management assessment.** Independent security risk- and gap-assessments from an attacker's point of view can determine your current security posture and risk profile. Be sure to consider the types of physical, cultural, operational, system and internal control breaches that innovative hackers and employees could perpetrate. It's vitally important to assess and test physical, cultural and technological controls in tandem.
- **Secure document-management system.** Replace traditional fax and e-mail systems with an integrated, secure document-management service that provides built-in fax and scanning capabilities, encrypted e-mail, version control and document delivery directly to your loan-origination system.
- **Physical security.** Ensure you have appropriate levels of physical security in place to limit access to sensitive data storage, data centers, network infrastructure and host systems. Outsourced LOS providers should provide a valid, independent SSAE 16 SOC-1 (Statement on Standards for Attestation En-

Continued >>

<< Continued

gagements report on service organization controls), which is a review of the provider's system and security practices performed by an independent CPA firm.

■ **Hiring practices.** Perform deep background and credit checks, as well as social media searches to identify potentially unfit employee candidates. Demand written explanations of any adverse data and consider whether the explanations are credible. Monitor employee compliance carefully in the initial period after hiring to identify potential issues.

■ **Network security.** Configure firewalls, enterprise class routing and switching equipment with appropriate security features such as access-control lists and virtual local area networks (VLANs) to isolate sensitive network segments. Configure network servers and hosts in a patched and hardened manner. Ensure you have proactive detection and monitoring of network anomalies and intrusions. Install a security information and event management (SIEM) device and tune it properly to detect attacks and worm breakouts in real time. Develop a formal incident-response plan and exercise it on a regular basis.

■ **Application security.** Configure your loan-origination system to secure sensitive client and loan data from start to finish. Assess "ease of use" versus "security" trade-offs. The careful deployment of user accounts with information-access controls often 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 also should allow the establishment of roles, rights and access views for defined parties. A senior executive should review user access and accounts, concentrating on employees with elevated access rights.

■ **Assess and test often.** Effective security requires careful and frequent risk assessments followed by well-designed testing. Testing should incorporate physical, logical and internal controls as well as social control testing. Virtually none of the system compromises described in this article were "brute force" attacks on a system or network; rather, most breaches occurred by employees circumventing established controls or hackers exploiting common weaknesses in the overall system of controls.

■ ■ ■

You never can have enough security, but as we have seen in the past few years, many financial companies have more work to do. The breaches described in this article occurred in banks and mortgage-banking companies that believed they had effective security measures in place. Following best practices can help mitigate many risks that can compromise your data. These are also the practices that state and federal examiners expect to be in place. ■