MORTGAGE Compliance
Magazine

# Data Security for Mortgage Companies: A Focus on Employees

Article by
Roshni Patel &
Daniel McKenna
December 2015

# DATA SECURITY FOR MORTGAGE COMPANIES: A FOCUS ON EMPLOYEES

BY ROSHNI PATEL & DANIEL McKENNA

Roshni Patel

Daniel McKenna

Whether you're with a mortgage broker, mortgage bank, or a vendor, companies that deal with mortgages collect more personal information than most retailers, service providers, and other financial institutions. A typical loan application requires reams of personal and confidential information. And all of this highly sensitive information has to be retained, in most cases, for the life of the loan. The risk of obtaining and holding large amounts of sensitive data is compounded by the fact that it is shared among the borrower, lender, vendors, attorneys, and other involved parties, some of whom may not be thinking about how to securely transmit or store it. With such risks, it is no surprise that the industry is a target for cybercriminals.

When you think of some of the biggest recent data breaches you may remember headlines about hackers, foreign cyber-espionage groups, and hostile foreign governments stealing sensitive data for nefarious purposes. Unfortunately, media coverage has sensationalized breaches and has caused many to overlook the leading cause of data incidents–employees. Employees have been, and continue to be, the number one cause of all reported data incidents. In some breaches, hackers gained access to networks by obtaining the login credentials of employees. In other breaches, it was malware-laced e-mail phishing attacks on vendor employees. Others were caused by fake requests to verify log-in information for social sites on the assumption that at least some employees were using the same password for both their work and social accounts.

But the most common of data incidents do not involve hacking at all. They involve human error and mistakes or malfeasance. Employees may accidentally leave laptops at a restaurant, put information on a thumb drive that is lost, print and remove documents they should not have access to, and send e-mails containing sensitive information outside of the firewall.

A company can spend millions of dollars on cybersecurity, yet still experience data incidents if a poorly-trained employee does something wrong. Fortunately, that risk can be minimized in a very cost-effective manner through proper policies, ➢

procedures, audit, and training. With what we have learned from past breaches and cybersecurity best practices in mind, we put together some tips to help companies in the mortgage industry identify and address employee risk factors that can lead to a data incident.

**1. Education and awareness are essential to cybersecurity.** Often the only information that employees receive about data security is during their new-hire orientation. While employees may remember this information for a while, over time they may forget the policies and procedures. On top of that, evolving threats and new technology require companies to periodically update their policies and procedures, but companies may forget to train employees on the updates. Companies should conduct regular training sessions for employees to teach them cyber and data security best practices and keep them aware of new and evolving threats. Make sure employees are aware of the relevant policies and procedures (and attest to reading and understanding them), know where to find them, and know what they should do if an issue arises.

**2. Remind employees to back up their data regularly.** Accidents happen–spilling a drink on a laptop, leaving a phone on the bus, clicking on the wrong link, and inadvertently downloading a virus. Having data backed up can save a lot of time and money. On a larger scale, backing up your company's important data may make the difference between carrying on and shutting your doors for good in the event of a natural disaster or cyber intrusion that causes a major data loss.

**3. Create an incident response plan and incident response team.** Often the most difficult and expensive time for a company is learning that an incident–even a lost laptop–occurred and determining the exposure and how to deal with it. Putting a plan in place allows your team to spring into action without delay or panic to resolve the problem and deal with any related issues. Having a set response team with pre-approved authority allows that plan to be implemented quickly and cost-effectively without the need for costly internal delays. This can be the one of the best time- and cost-saving decisions your company makes.

**4. Require good password practices.** Hacking can be facilitated by something as simple as someone guessing the password to an employee's computer and logging on to download sensitive data. To make this less likely, remind your employees of these best password practices:

- Never keep the manufacturer- or developer-provided default password;
- Change passwords often and do not repeat passwords if possible;
- The longer the password the better, but do not use personal information or common phrases in your password; and
- Make passwords a combination of lower- and upper-case letters, numbers, and symbols.

**5. Password-protect anything and everything.** Many people do not like entering a password or PIN every time they want to use their phone; but, if the device accesses company information, it is a requirement. Mobile devices can be shared with others or easily lost, exposing sensitive information to unintended parties. Phones, tablets, computers, and any other device that allows it should be protected with a password or PIN. This rule is particularly important for company-owned devices. A study of breaches affecting the financial industry reported that approximately 18 percent of the breaches were caused by theft of company servers, external hard drives, and employee laptops.[1]

**6. Patch your software and keep your antivirus and anti-malware programs up-to-date.** Vulnerabilities are being discovered every day, and, in response, software developers and security professionals regularly release patches and updates. Keep track of these developments and make sure that you have a system in place to implement them. Also make sure that employees know to update the software on their personal devices. Most hackers use known weaknesses to exploit systems that have not been updated. Requiring regular updates significantly reduces your risk of loss.

**7. Create policies and procedures for employees working remotely.** Employees that work outside of the office may not want to ask for a secure means ▷

of remote access to the documents that they need. Instead, they may come up with their own solutions, such as printing electronic files or downloading files to an unsecured personal hard drive. You would not allow employees to walk around with a briefcase full of loan applications. You similarly should not allow thumb drives or e-mails filled with sensitive information. Consider supporting a Virtual Private Network (VPN) to create a secure Internet connection from a remote location to your company's network so that employees can securely access the files that they need. Make sure employees are trained and encouraged to use the VPN software. If you choose to allow remote access without a VPN, ask employees to use secure wireless networks whenever possible and always when they are dealing with sensitive company information. Public wireless networks are more vulnerable and can put you at risk of being hacked.

**Significantly minimize that risk by following these tips to avoid some of the most common pitfalls that have led to data breaches.**

**8. Train your employees how to securely transmit files.** In January 2014, HALOCK Security Labs released the results of an investigation of 63 U.S. mortgage lenders. The company found that lenders often prioritize customer convenience and comfort over data security. Only 12 percent of the lenders offered borrowers a secure e-mail portal to transfer files.[2] Client portals allow both borrowers and lenders to upload sensitive documents to a secure website, where each has a password and log in to retrieve the documents. Creating a client portal and training and encouraging employees to use it whenever sensitive information is involved will mitigate risk in data transmission.

**9. Educate your employees about spam and phishing.** Teach them how to spot malicious e-mails and websites, what common tricks and methods hackers use to obtain personal information, and how to report a suspicious e-mail to your IT department so they can stop others from falling victim to it. Remind employees to be careful when clicking on attachments or links in e-mails and to double-check the URL of website links. A misspelled word in a URL can indicate a link to a harmful domain.

**10. Know that employees will occasionally be responsible for data disposal and teach them how to do it.** Many people replace their phones, laptops, and other mobile devices every two to three years. Your employees may think that all they need to do is delete files from their phones before selling them online, but data can be recovered if it is not correctly destroyed. Teach employees the best ways to remove sensitive data from their devices once the data is no longer needed. For company-owned devices that are no longer being used, you may consider hiring a professional to make sure that sensitive data is properly deleted.

Unfortunately, companies also need to protect against data breaches connected to corporate espionage or simple theft as insider breaches have been reported at a number of mortgage companies.

Although it is difficult to predict whether an employee will steal or otherwise misuse your company's sensitive information, there are a few things that you can do to protect your records.

**1. Limit access to confidential information.** Make sure that employees can only access the information that they need to perform their job functions. A Ponemon Institute study released last year reported that 71 percent of employees surveyed believed that they had access to confidential company data that they probably should not see. Of those employees, 38 percent said that they have seen "a lot of data."[3]

**2. Remind employees to use common sense.** Even if an employee chooses a strong password, simple mistakes can reveal that password to malevolent parties, including co-workers. Common sense means making sure that no one is watching them while they type out a password; not sharing their password with others, including co-workers; not keeping a list of their passwords; and, if they must keep a list, keeping it in a secure location, such as a locked drawer. Employees should be reminded to use different passwords for their personal and work accounts. Similarly,

they should not use the same password for all of their personal accounts or all of their work accounts.

**3. Be on the lookout for non-approved software.** Allowing employees to download and use whatever software they want opens up your network to unnecessary risks, such as the introduction of malware from infected installation software or the unencrypted transmission of sensitive data. Make sure employees know the policy on software installation and what software your IT department has approved. Also, make sure your IT department monitors what software employees are downloading and using.

Of course, it is impossible to completely obviate cyber and data security risks. But, you can significantly minimize that risk by following these tips to avoid some of the most common pitfalls that have led to data breaches. MCM

---

Roshni Patel advises clients on privacy and data security matters, including permissible data collection, use, and sharing practices for mobile apps, Safe Harbor certification, and compliance with laws, regulations, and industry guidelines. Ms. Patel helps companies develop strong privacy and data security policies and procedures. Roshni can be reached at: PatelR@ballardspahr.comvellit

Ballard Spahr partner Daniel JT McKenna devotes his practice to privacy and data security, consumer financial services, and mortgage banking litigation. Daniel can be reached at: McKennaD@ballardspahr.com

---

[1] *Common Data Breach Threats Facing Financial Institutions*, BEAZLEY BREACH SOLUTIONS (Feb. 25, 2015), https://www.beazleybreachsolutions.com/Documents/Prepare/Security/CommonDataBreachThreats_FI.pdf.

[2] HALCOK Security Labs, *Some Mortgage Lenders May Be Putting Sensitive Financial Data at Risk, Finds HALOCK*, HALOCK BLOG (Jan. 29, 2014), http://www.halock.com/blog/halock-investigation-finds-70-mortgage-lenders-putting-sensitive-financial-data-risk-application-processes/.

[3] PONEMON INSTITUTE LLC, CORPORATE DATA: A PROTECTED ASSET OR A TICKING TIME BOMB? 3-4 (2014), *available at* http://info.varonis.com/hs-fs/hub/142972/file-2194864500-pdf/ponemon-data-breach-study.pdf.