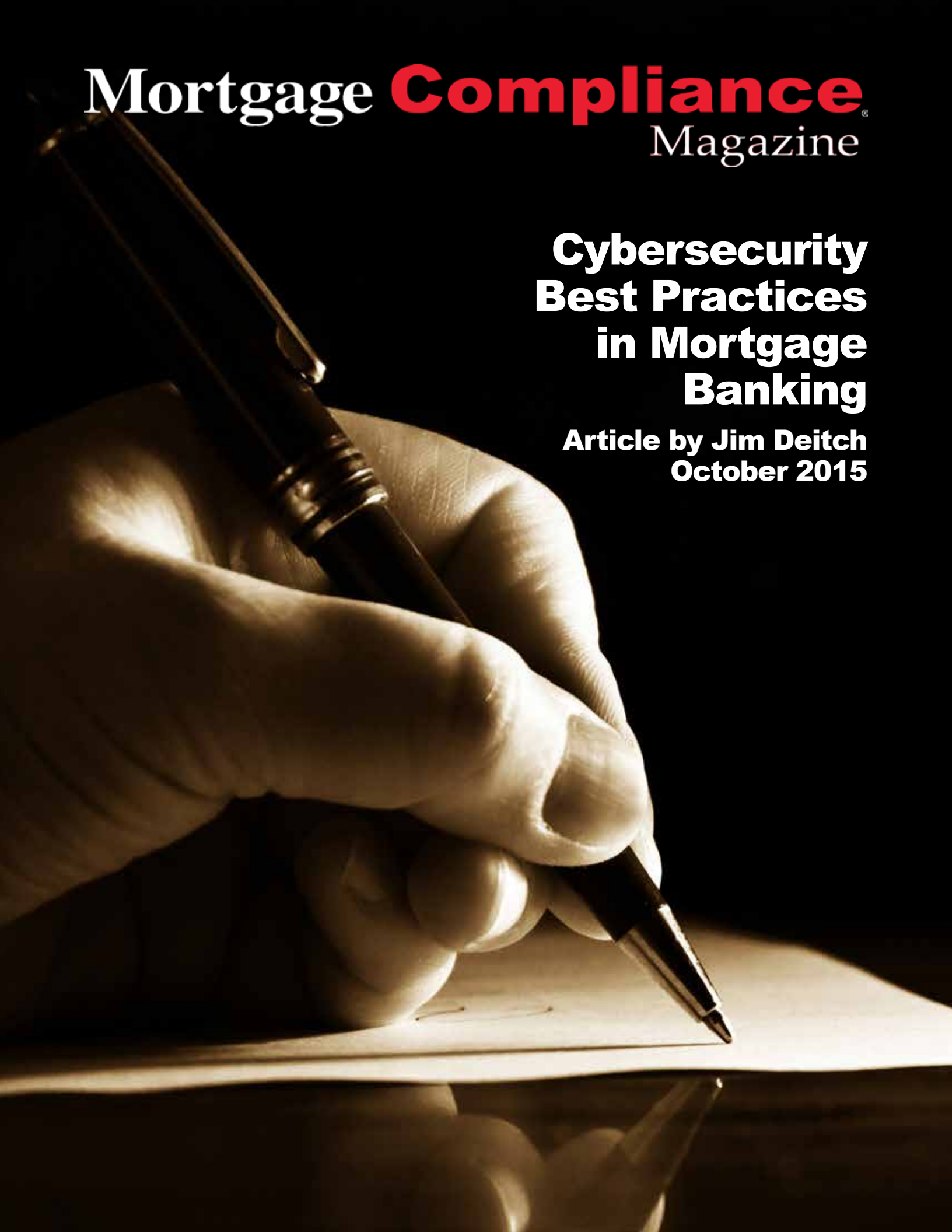
Mortgage Compliance Magazine



Cybersecurity Best Practices in Mortgage Banking

Article by Jim Deitch

October 2015

Cybersecurity Best Practices in Mortgage Banking

BY JIM DEITCH

Jim Deitch

Recent high-profile cyberattacks have clearly demonstrated the financial, operational, legal, and reputational damage such attacks can have on financial institutions.

The Federal Financial Institutions Examination Council (FFIEC) issued its Cyber Assessment Tool on June 30, 2015. The FFIEC is comprised of members from the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the Federal Reserve Board (FRB), the National Credit Union Association (NCUA), the Consumer Financial Protection Bureau (CFPB) and the State Liaison Committee of State Regulators.

During the summer of 2014, the FFIEC piloted a Cybersecurity Assessment (Assessment) at more than 500 community financial institutions. These assessments provided a baseline for various regulators to evaluate banks' preparedness to identify and mitigate information security (IS) risks.

The Assessment was undertaken due to the increasing volume and sophistication of cyber threats and the risks that cyber threats pose to the national banking infrastructure, banks, lenders, businesses, and consumers. Recent high-profile cyberattacks have clearly demonstrated the financial, operational, legal, and reputational damage such attacks can have on financial institutions. Costs include forensic investigations, legal fees, consumer credit monitoring, technology changes, public relations campaigns, and reputational damage.

The Cybersecurity Assessment Tool is a framework for financial institutions and mortgage lenders to identify IS risks and determine their cybersecurity preparedness. The Cybersecurity Assessment Tool provides a repeatable and measurable process for financial institutions and mortgage lenders to measure the inherent risks associated with their business model. It also provides a methodology to measure the cybersecurity maturity of the institution or lender, and assess whether the cyber maturity level is appropriate for the inherent risks of the particular business model.

Another reason to use the Cybersecurity Assessment Tool is embodied in a recent court decision. The recent decision of the U.S. Court of Appeals for the Third Circuit giving the Federal Trade Commission (FTC) authority to penalize the Wyndham Hotel chain for inadequate cybersecurity will mean an increase in FTC and other regulators' enforcement actions, including lawsuits. Despite a lack of clear regulations, the Third Circuit gave the FTC latitude to determine when a lack of adequate cybersecurity can be considered an unfair, deceptive or abusive act or practice (UDAAP).

The CFPB will certainly take note of this litigation, as a federal appeals court

has suggested it appropriate to charge any financial services company with a UDAAP issue if a breach occurs, or potentially even without a breach. Given this, it is critically important to establish a credible position that the data security in place is consistent with best practices and recognized data security standards. The FFIEC Tools are not a "safe harbor," but lack of due regard for them will almost certainly be used against a bank or lender if a breach occurs or an examination cites weak IS practices.

How might a bank or lender approach the FFIEC Tools? Regulators do not expect a bank or lender to use the Cybersecurity Assessment Tool as a "check the box" exercise. Consider the Cybersecurity Assessment Tool as a starting point, to be customized to the bank or lender's circumstances. For instance, the Cybersecurity Assessment Tool does not highlight that many mortgage lenders use outside loan officers. These loan officers often use Wi-Fi connections in realtor offices, businesses, coffee shops, and other unsecure locations. The Cybersecurity Assessment Tool must adapt to the context of the bank or lender's business model. Many mortgage lenders permit loan officers and loan production offices to "Bring Your Own Devices" or BYOD. BYOD presents a variety of IS risks, including the use of a variety of non-standard devices.

It's very important to realize that IS is not a CIO's responsibility. Former Governor Tom Ridge, CEO of Ridge Global, an international IS firm, and former Secretary of the Department of Homeland Security described a situation: "We worked with a company that had significant relationships between their operational technology people and their information technology people. When we recommended they sit down and hold more in-depth meetings to really make sure that their respective areas of the company are integrated in terms of cybersecurity they asked 'Why would we want to do that?' So, you really want to break down those silos."

It's important to consider an enterprise-wide approach. Governor Ridge continued: "[Your Company] is probably going to be breached. Do you have an incident response plan? Who will you call to deal with the breach from the technical side? How are you going to deal with regulators? How are you going to deal with the public? Do you have a communications plan? You have to assume there is going to be a breach."

The Cybersecurity Assessment Tool is a starting point, but consider how to incorporate the following questions in your bank or lenders' assessment:

Consider a Data and Risk Inventory: What Personally Identifiable Information (PII) does the company collect? Where and how is data stored and segregated? Is the PII stored on digital copiers, laptops, tablets, phones, mobile apps? How is very sensitive data protected (i.e. is it encrypted)? How is data used? How is data disposed of, and when? What controls are in pace to protect access to data (i.e., dual authentication)? Remember that PII can be in the memory of copiers, employee phones, and other areas that may not be obvious.

Ensure the bank or lender's Security Incident Response Policy defines what a 'breach' is. The high profile breaches with large volumes of PII are obvious (think Office of Personnel Management, Target, Anthem). But what about an incident where a loan officer downloads his customer list of 1,200 names and addresses and a pipeline report listing income and credit information and takes it to a competitor? What about a Loan Origination System reporting database containing PII that appears to have been entered by a hacker, but it is unclear by whom and whether information was extracted? How about a situation where a loan officer clicks on a Phishing email and a 'CryptoLocker' malware locks company files and demands a ransom? What about when a disgruntled employee posts former customer PII on the 'dark web'?

Collaboration among executives across business lines can better define what a breach is and what to do about it. Collaboration in advance can define who is in charge of data privacy--the CIO, Legal Department, Compliance, COO, or the CEO? It can define the difference between a 'security incident' and 'data breach' for the entire company. Make sure your entire management team is aware of the Incident Response Plan. Will you engage legal counsel at the beginning, and if so, which executive will engage counsel, and who will be used? When will your company contact law enforcement personnel, and who will contact them?

Federal and state regulators require different responses to a breach. Which data privacy laws apply to your collection and use of the data? State laws are usually enforced by the state attorney general and typically deal with things like notification requirements in the event of a data breach. Federal laws ➢

(Graham-Leach-Bliley) apply to protection of PII. Be sure to inventory state requirements and make certain when they apply. Failure to notify state regulators and failure to notify consumers in accordance with state laws can amplify enforcement actions, reputational risks and monetary damages. Determine referral and notification policies to law enforcement beforehand. Prepare for the consumer and regulatory notification process. Know what identity theft and other damages your clients may face. Plan for remedies to be offered to clients -- fraud security measures at a minimum.

Note that the FFIEC Cyber Maturity Baseline Assessment lists the federal examination manual and regulatory citations regarding each element of cyber maturity. The higher maturity levels do not cite the exam or regulatory citations. This means that the FFIEC (and its constituent regulators) regard the 'baseline' maturity as the minimum IS elements necessary. Does failure to meet the FFIEC baseline standards suggest a UDAAP? If a bank or lender doesn't meet the cyber maturity baseline, does a comprehensive remediation plan constitute an effective mitigant as maturity is improved?

Banks and lenders use a large number of vendors. How do vendors protect your company and your customers' data? Do the IS and privacy requirements of your vendors align to your IS requirements? Each vendor you do business with should have a comprehensive vendor management response document, and should carry data breach insurance.

Do you have cyber Insurance? Data breach costs can mushroom quickly. Costs of each lost record could range from $10-$200. Things you need to think about include how much personal data the company processes? What would be the harm of a data breach to the company's reputation? What is a reasonable cost per record lost? What if the business is materially interrupted in the event of a breach? What will consumers expect the company to do in the event of a breach (e.g., credit monitoring)? Among other considerations.

A careful and collaborative risk assessment and a thoughtful Cyber Maturity Assessment using the FFIEC tools is a valuable exercise that should be frequently repeated.

CYBERSECURITY "BEST PRACTICES"

Hackers know the typical security implementations of CIOs. Therefore, a key element of effective IT security is to approach it from a hacker's perspective. Most lenders have very good 'perimeter security,' such as firewalls and related appliances; yet, this is not how hackers typically gain access. Virtually every breach reported publicly did not occur by a direct attack on traditional perimeter security. Allen Harper, Chief Hacker at Tangible Security, suggests that up to 80% of initial entries into systems are accomplished by 'social engineering.'

Social engineering is any technique designed to trick an employee (or trusted vendor) into providing access to an IT system. Social engineering breaches include clicking on attachments to Phishing Emails, visiting and navigating on websites designed to introduce malware through a browser, phone phishing for sensitive information, Business Email Compromises, and a host of other methods.

Examples of social engineering include multiple CryptoLocker invasions of a mortgage lender, a Business Email Compromise to obtain and redirect a business wire transfers to a hacker, and a Spear Phishing email compromise to divert borrower down payments from a closing agent to a crook. 'Spear Phishing' is targeting a specific company or individual, versus Phishing, which is simply casting a broad net to potential targets. Spear Phishing is becoming more dangerous, as an email directed to a target usually is crafted to appear legitimate and to request action on a routine function, such as wire transfers.

At the forefront of IS are two inexpensive protections. The first is employee training. The key is to educate employees on typical social engineering schemes, test employee compliance on a regular basis, and encourage employees to immediately submit an incident report if they suspect that they may have opened a suspicious email or attachment, or visited an infected website.

The second important security measure that a banker can take is to ensure that 'patches' issued by the software maker are installed as soon as they are released. Most computers can be configured to automatically install software updates and patches. Patches for servers, routers, and other devices must usually be installed by the bank's IT team. In some cases, users disable automatic updates and place their computers in harm's way. Banks and lenders must develop and implement a corporate standard for deploying patches to all systems in a timely manner. Unpatched

systems are open invitations to hackers, exploits and IS incidents.

Additional tools to increase the likelihood that a bank or lender IS Program likely meets FFIEC and state regulators' requirements include:

1. Robust security testing including ethical hacking, multi-vector attacks on various attack surfaces, from both outside and inside the company's perimeter.
2. Data encryption and criteria around the types of data to encrypt.
3. Formal Security Incident and Event Management (SIEM) policies and protocols.
4. Documentation of data monitoring that is in place.
5. Documentation and review of outside vendors and partners and their security safeguards, procedures, and controls.
6. Identification of all hardware devices attached to the company's networks and software on devices. Mapping and monitoring every node is a must.
7. Plans for restoration of operations if an attack should take place.
8. Effective data backup: frequency, types, multiple types of backup, and hot backup sites.
9. Business continuity plans.

The IS regulatory environment has changed with the issuance of the FFIEC Cybersecurity Assessment Tool and the FTC v. Wyndham case. The need for a collaborative and robust IS program is more important than ever. The best IS programs involve broad employee education, a collaborative approach among executives, and constant testing, assessment and remediation of possible shortcomings. MCM

James M. Deitch is CEO and Co-Founder of Teraverde. Mr. Deitch is a thought leader in community and mortgage banking, having served as CEO of 4 community banks, including 2 de novo banks. James can be reached at jdeitch@teraverde.com.