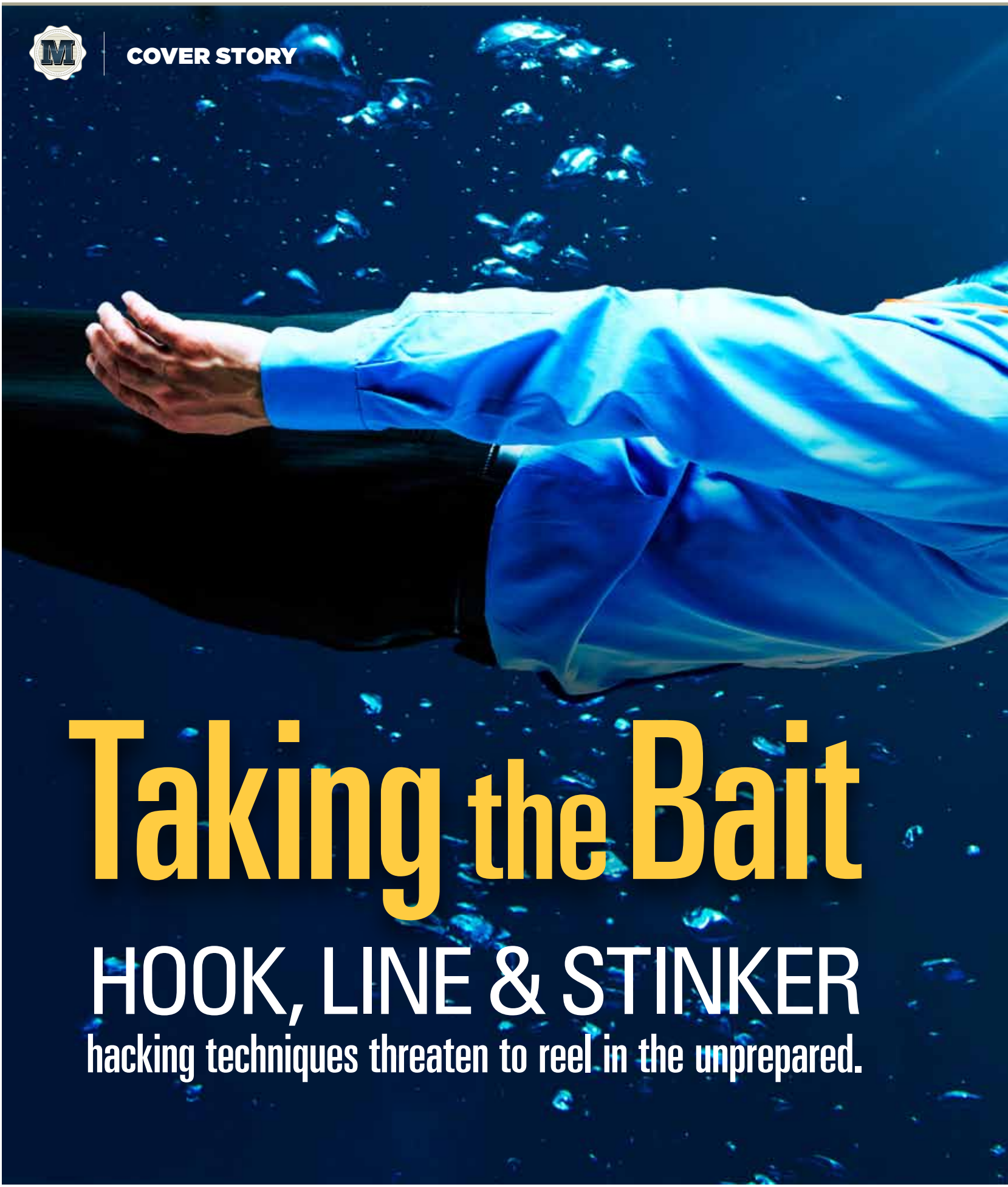

Taking the Bait

HOOK, LINE & STINKER

hacking techniques threaten to reel in the unprepared.

By Tory Barringer

If you've somehow made it through the last few months without hearing about Heartbleed, now might be a good time to acquaint yourself.

The security flaw—exposed in early April by Google Security and a team of engineers at cybersecurity firm Codenomicon—affected certain versions of OpenSSL, altogether impacting about two-thirds of active Internet servers today. Put simply, it left open a hole for attackers to pull user credentials and encryption keys themselves, leaving vast amounts of data potentially up for grabs.

Heartbleed isn't the only security glitch to show up in the news lately. Mortgage tech followers might remember another incident in early April, when Ellie Mae made headlines following a system outage "consistent with an external malicious attack characteristic of a distributed denial of service (DDoS)"; in other words, the company's network was flooded with enough information at one time to trigger an overload.

(Days later, Ellie Mae revealed the downtime was caused not by attackers but rather by an unexpected jump in demand at the end of March. Despite the fact that no attack was made and no data breached, in the company's latest quarterly earnings report, CEO Sig Anderman revealed Ellie Mae has committed funds to bolstering its infrastructure, security included.)

If there is a silver lining to stories such as these, it would be the conversation that's ensued about security in the face of rapidly changing technology. As more mortgage firms become growingly dependent on automated solutions and electronic file management, national reports about issues like Heartbleed shine a spotlight on the importance of making sure those packages of borrower information—virtual treasure chests for hackers—stay private.

Waiting for a Wake-Up Call

Who suffers most in the event of a data breach? Undoubtedly, there's a lot at stake for the average American whose financial details have been left unprotected, but there's just as much risk for the company that failed to do any protecting.

Unfortunately, just as it is with consumers, too many organizations are happy to push security concerns to the back burner until a highly publicized breach forces them to wake up. Allen Harper, EVP and chief hacker for cybersecurity firm Tangible Security and author of Gray Hat Hacking: The Ethical Hacker's Handbook, calls these types of high-profile incidents "CNN-level events."

"They just haven't experienced a CNN moment," Harper said. "Somebody's going to have to be made an example of, and they're all kind of hoping it's not them."

Rather, he says, the mortgage industry—like many others—has adopted a largely "if it isn't broke, don't fix it" stance regarding security, whether it's because of costs or complications.

A perfect demonstration of that mentality can be found in a recent investigation from HALOCK Security Labs, in which the security company found that 70 percent of lenders nationwide—including a majority of the country's top lenders—allow mortgage applications to send their personal and financial information through unencrypted email channels or faxes. Asked why they don't offer a secure email portal to applications, many respondents reportedly said it was simply a

How Do Regs Fit In?

As if normal security considerations weren't enough to deal with, finance businesses also need to be sure their efforts will hold up under regulatory scrutiny. Federal laws governing consumer privacy are nothing new, but with the recent series of high-profile incidents, agencies like the Office of the Comptroller of the Currency (OCC) and the Consumer Financial Protection Bureau (CFPB) are casting a focused eye on financial institutions and privacy practices, particularly when it comes to third-party vendor relationships.

"[Lenders] have to think of it two ways," said Christopher Gulotta, CEO and founder of Real Estate Data Shield and the Gulotta Law Group. "They have to think, 'What do we need to do to show we're compliant,' but they also have to know their vendors are screened, monitored, [and] secure."

Adding to the complexity is that regulators actually left a good deal of discretion to companies to monitor their own privacy efforts and decide if they think they've taken reasonable steps under the law. While that approach is flexible on the government's part, Gulotta says it's really just created a confusing environment:

"I think the regulators were trying to be fair to corporate America and say, 'Hey, just do what's appropriate.' [But] this has created a lot of concern in the industry because small banks and big banks have to decide, 'If we suffer a breach, will they decide we didn't do enough?'"

To simplify matters, he recommends following an easy acronym in going down the checklist: RADDCO, or Risk Assessment, Due Diligence, Contracts, and Oversight.

matter of convenience, with one anonymous respondent remarking, "Oftentimes it was easier to have my clients send documents like W-2s through email because everyone has access to an email account. Most of us [lenders] didn't want to take the time to explain what a secure portal was and how to use it. Everyone understands what email is."

However, that focus on ease of use can often come back to hurt companies when they have to explain to the public how their customers' data was compromised, explains James Deitch, CEO and co-founder of Teraverde, a consulting firm for the banking and financial industries.

"Customers are beginning to ask: 'Is my data secure, and do you have the capability to protect my data?'" Deitch said. "And that question has to be answered by the loan officer, and it has to be answered with real affirmation."

And if a company does drop the ball on the security front? For an example, look at Target, which recently lost its CEO and took a hit to its fourth-quarter earnings as a result of a high-profile breach announced just weeks before Christmas last year. While the retailer's first-quarter report was unavailable as of press time, analysts have set their sights low as the fallout continues.

"Reputationally, once you get a black eye, it's awfully difficult to recover," Deitch said.

Know Thy Enemy

So how does a careful company prepare its defenses against hackers? By putting hackers to work for them, of course.

As part of its offerings, Tangible conducts penetration tests, moving on clients' systems the way a malicious attacker might move and reporting back with its findings—what those in the industry call an "adversarial approach." While Harper was initially surprised by the amount of data he could extract on a routine basis, he says it's actually alarmingly common for the company to easily get anywhere a hacker would want to go.

"We always get to the money. It's amazingly simple and easy. We're not shocked by it anymore, but the clients often are," he remarked.

Making matters worse is the fact that many companies simply don't know how vulnerable they actually are. What happens all too often, Harper says, is that businesses will pay for the cheapest, least thorough penetration test available, resulting in little progress made on the tester's end and a false sense of security for the company.

In fact, he says, a good way to tell the difference between a cheap penetration test and a thorough probe is the results you end up with. If your hired "attacker" turns up with too little, there's a chance you're not getting the kind of comprehensive analysis you really need.

"Customers are beginning to ask: 'Is my data secure, and do you have the capability to protect my data?'"

—**James Deitch,** Teraverde.

Inside Man

Of course, not all breaches are solely the result of an outsider attack. Like in every heist movie, some of the biggest scores start with someone on the inside: a disgruntled former employee who still has access, an improperly screened loan officer with a criminal record, or an unaware worker who is granted too much access and doesn't know what to do with it.

In fact, in a recent white paper released by Teraverde and Tangible, co-authors Deitch and Harper describe more than a dozen different data breaches—many of which are the result of untrained employees and improper protocols.

"The headline news is about hackers that brute-force their way into a high-profile target," Deitch said. "The reality is that most of the security breaches that we come across have been what I call either poor execution of a policy or deficient policy to begin with."

In one of the more egregious scenarios described, "a bank employee with a laptop inserted an infected USB thumb-drive file, causing complete laptop compromise, which a hacker used to obtain complete network compromise, including LOS application, customer data breach, and a gateway into other bank systems in a federally insured bank." All of that from a device many people keep on their keychains.

If a typical employee can cause that kind of chaos without intending to, imagine the damage that could be done by somebody leaving for another company. For that matter, consider the number of people filtering in and out of a typical workplace every day: the person who fixes the copier, the person who restocks the water cooler, the building custodians, and so on.

"A lost of trust is given to vendors," Deitch said. "In some

aspects, it just doesn't occur to the executives that a simple thing like being very, very serious about restricting physical access to the premises at lenders can be as important as it is."

Another type of threat comes from what security experts like Harper term a "drive-by attack": a worker happens to be surfing the Internet on an unpatched browser with a major security flaw. They happen to go to the wrong site—whether it's a mortgage banking site or otherwise—and now they've pulled in an attacker by accident, giving the wrong people "insider status." Wrong place, wrong time: drive-by.

"Because of the threat environment that we face on the Internet, all of our users are just one click from essentially becoming a malicious insider themselves," Harper explained. "It doesn't mean much if most of those security issues have to be found on the inside, because attackers get in very easily."

Creating a Barrier

Facing so many threats from within and without, it might seem impossible to ensure an airtight operation. However, while "airtight" might in fact be a guarantee no company can make, there are easy steps to limit the risk of a breach. The most obvious (and cheapest) one? Education.

Many of these problems, explains HALOCK SVP Terry Kurzynski, stem from a simple lack of understanding: "It's just a complete ignorance of the real liability, not really knowing how to do anything about it—'We're not security, we're not technology people, we just process loans,'" he said.

Thankfully, that's easy enough to deal with through training and proper configurations on all technologies in use. By limiting data access to only those employees who need it (and limiting those employees to only what they need for their job), businesses can go a long way toward keeping their customers' private data exactly that—private.

The only thing stopping most lenders from taking that step, Kurzynski says, is their own self-placed limitations.

"When you think about it, a lot of these lenders are fairly small," he said. "They just really don't have the resources to say, 'We're going to do something about this,' not knowing that it's actually fairly simple."

The alternative, of course, is far more complicated—and expensive. Said Harper, "You might be setting yourself up for a call from a reporter someday when you're on the other side of that CNN event." **M**