Established 1872 *Reprinted from the issue of February 13, 2012* www.BankerandTradesman.com

BANKER & TRADESMAN

THE REAL ESTATE, BANKING AND COMMERCIAL WEEKLY FOR MASSACHUSETTS

A PUBLICATION OF THE WARREN GROUP

COMPLIANCE CROSSROADS

BREACH OF FAITH

Loss Of Customer Personal Information Damages Banks' Credibility

Smart Businesses Minimize Opportunities For Theft Of Sensitive Data

BY MICHELLE DROLET
SPECIAL TO BANKER & TRADESMAN

On Jan. 5, federal law enforcement seized several automobiles worth about $100,000 in value. They had belonged to the former president of the Massachusetts Bank and Trust Company and were taken as restitution for his defrauding the bank in 1997. It seems that not a day passes by when news of banking-related fraud, money laundering, or a privacy violation is reported.

MICHELLE DROLET

Last year in May, Bank of America sustained a $10-million loss when an insider sold the bank's customer data to organized criminals who then committed fraud against the bank's customers. Thanks to a former associate, the scammers obtained names, addresses, Social Security numbers, phone numbers, bank account numbers, driver's license numbers, birth dates, email addresses, mother's maiden names, PINs and account balances.

All organizations depend on information. Confidential information – sales leads, customer accounts, trade secrets, intellectual property (IP) – gives you the competitive edge. If that information is stolen or misused, however, your competitive edge can evaporate and your reputation and balance sheet can take a major and potentially fatal hit.

Lax Monitoring

Regulated information – such as credit cards, personal and financial informtion – is frequently the target of attacks. Theoretically, this data is protected by U.S., state and federal regulations that require strong security controls.

The reality, however, is that many businesses are not fully compliant with these regulations. Or, they may believe they are – with all the right policies in place, but lax or no monitoring or enforcement.

It doesn't matter how regulated data is lost – whether a hacker steals customer data, or a well-meaning employee loses a laptop or other portable

continued on page 2

device containing sensitive data. Whatever the cause, the loss of regulated information amounts to a reportable data breach.

Recently enacted state and federal regulations mandate security breach reporting if it involves customer or employee personally identifiable information (PII). But the increase in breaches can't be accounted for by increased reporting alone.

Key Chains To Disaster

We've all seen it: Critical information is backed up on USB drives that dangle at the end of key chains. Employees increasingly depend on devices that IT has little or no control over, such as smartphones, tablets and MP3 players. Users often back up sensitive data to these gadgets – and often fail to encrypt it, compounding the impact of its loss. Some banks prohibit employees from using USB drives, but most have no formal policy in place.

Tangible losses are those for which we can calculate a cost. But intangible losses – particularly the loss of trust – can't be fully measured. Trust takes time to build. And it can be wiped out in an instant when a trusted organization loses or misuses the personal information that has been entrusted to it. This is particularly true for customer information loss.

The loss of any information – whether internal confidential communications, customer and employee information protected by regulations, trade secrets or intellectual property – is costly in tangible and intangible ways.

It doesn't matter how regulated data is lost – whether a hacker steals customer data, or a well-meaning employee loses a laptop or other portable device containing sensitive data. Whatever the cause, the loss of regulated information amounts to a reportable data breach.

Even if your organization doesn't outsource, you're still at risk for a more common type of insider attack – customer information theft. Bank of America, JPMorgan Chase, UBS AG, Wells Fargo and General Electric have publicly acknowledged that former employees engaged in illegal activity. The companies have paid a combined $743 million in restitution and penalties.

Gray Area

Unlike piracy or patent infringement, customer information theft exists in a legal gray area. In many states, non-compete and non-solicitation agreements favor the organization. But in some states non-compete clauses are not enforceable. The employee can retain the relationship so long as it doesn't involve any solicitation. These terms and conditions are nearly impossible to enforce.

When departing employees take sensitive organizational data with them as they leave, the potential for negative consequences is enormous. If you suspect an employee has improperly taken customer information, you need a strong forensic process and tools in place, as well as policies that prevent, for instance, the re-issuing of computers the moment someone leaves. Otherwise – you'll be hard-pressed to prove any wrong-doing.

One way of minimizing insiders' opportunity to steal sensitive data is through vulnerability scanning and penetration testing. These can help your organization find weaknesses in access controls, the technical implementation of administrative policies and other vulnerabilities that enable insider attacks. ■

Michelle Drolet is founder and CEO of Towerwall, an IT security services provider in Framingham.
Email: michelled@towerwall.com.