CHICAGOLAWBULLETIN.COM

Serving Chicago's legal community for 159 years

MONDAY, JUNE 23, 2014

Chicago Daily Law Bulletin®

Volume 160, No. 123

To keep data safe, law firms must embrace a culture of security

As the White House report on big data indicates, an enormous amount of information is collected, stored, analyzed and relayed in digitized form over the Internet and, increasingly, using mobile technology.

Headlines continue to focus on consumer data security against the backdrop of yet another security breach.

While Target is still attempting to recover from the December 2013 attack which compromised the credit and debit card information of 40 million consumers and the non-financial information of another 70 million, the press is now reporting about another data breach at eBay in which hackers stole the login credentials for a number of the company's employees and eventually used them to steal the personally identifiable information of eBay users, including names, addresses, phone numbers and birthdates as well as encrypted passwords.

But it is not just consumer retailers that need to worry about data security. All businesses — even those that don't collect or process consumer financial data — are vulnerable to data breaches.

In addition, and as illustrated by the Target and eBay violations, among others, hackers are often able to gain access through a weak point or security "blind spot," whether from within the company or outside — through a third-party vendor, for example, as was the case with the Target breach.

Surprisingly, while attorneys and law firms advise clients on privacy and data security compliance and post-breach mitigation, law firms may inadvertently be a third-party vendor compromising their clients' data security. By failing to take adequate measures to secure their own sensitive client information, law firms may be the weak link in the data security ecosystem.

In one recent study by LexisNexis, the vast majority of the 300 law firm respondents — 89 percent — conveyed information and documents through unencrypted e-mail, and 77 percent rely on the confidentiality statement at the bottom of those e-mails as their only means of "protecting" confidential information and attorney-client communications.

Only a minority of firms report using security technology to protect electronic communications, including e-mail encryption (22 percent), password-protected documents (14 percent) or a secure file-sharing site (13 percent).

Mobile technology increases these risks and poses new ones. Many attorneys regularly use applications on smartphones and tablets to conduct business and communicate with clients and colleagues.

By failing to take adequate measures to secure their own sensitive client information, law firms may be the weak link in the data security ecosystem.

But as the Federal Trade Commission pointed out in its recent blog post, "Business execs: 7 things to consider before using that app," many business people (including lawyers) use these applications to transmit sensitive customer, client or employee information without knowing what, if any, security precautions the app provides.

And while many apps claim to secure the data, the FTC notes some apps don't deliver on those claims. Because mobility may be key to client service, mobile phones, tablets and apps are unavoidable, and law firms must develop policies to ensure that attorneys and staff use mobile devices in ways that minimize the risk of unauthorized access to confidential or sensitive information — whether inadvertent or as the result of deliberate attempts by hackers.

Hackers use malware to gain entry into their targets' systems. Law firms should enact technology policies that will minimize the risk of contracting malware through mobile applications.

Attorneys and staff must remember that mobile devices for business use (as well as personal uses) are computers and should exercise the same precautions they would with office computers and laptops.

Acceptable-use policies should include the following:

•A requirement that users only use computers and mobile devices on secure networks. Systems can be compromised when users access the Internet through "open" Wi-Fi networks, such as those offered at airports and coffee shops.

•Mobile devices should be configured to their full security settings with secure password protections.

•Mobile devices should be fully encrypted with strong passwords that users are required to change on a regular basis.

•Users should be reminded never to "jailbreak" their devices or take other measures that would reduce the security of their device.

•Users also should keep their systems up-to-date, installing updates not only to their operating systems but to any installed applications.

•Requirements related to the selection and downloading of apps. As the FTC suggests, users should be especially careful in selecting apps and should only download apps after understanding the security policy, including what data the app is seeking and how that data will be protected. An app that asks to access information beyond that which is strictly necessary for the app's function should be considered suspect. When in doubt, don't download.

•Requirements related to the use of cloud storage services. Firms should also consider policies concerning the use of cloud storage services, building a secure cloud-based service or providing guidance to employees concerning approved uses.

In addition to acceptable-use policies for mobile devices, the law firms and attorneys might

PRIVACY, TECHNOLOGY AND LAW

NERISSA COYLE MCGINN

Nerissa Coyle McGinn is a partner in Loeb & Loeb's Chicago office. She focuses on matters involving the convergence of advertising and promotions, emerging media, technology and privacy law as well as intellectual property law. She can be reached on nmcginn@loeb.com.

take several other, broader lessons from recent data breaches.

In the Target breach, the hackers' accessed the company's servers through credentials stolen from an HVAC systems company that reportedly used Target's system credentials to manage a number of processes remotely.

Law firms act as third-party service providers to their clients and, in providing that legal service, law firms often employ other third-party vendors and consultants. Regardless of the technical specifics of the breach, the takeaway is clear: Companies (including law firms) need to be diligent in selecting any outside parties that may have access to their networks and systems.

That would include electronic payroll systems, outsourced billing services, cloud storage providers, IT service providers or consultants and any other third-party vendor with access to the firm's networks and data.

While no individual or entity is entirely immune to security breaches, law firms should strive to not only ensure that their internal security measures are robust but also that any outside vendors or service providers employ appropriate security measures, including physical precautions, such as keeping servers in secure (locked) environments as well as technical measures, such as the use of strong encryption technology.

Law firms should treat outside service providers as part of an integrated system, taking care to ensure that all the "spokes" that lead to the hub — the client — observe rigorous security measures.

The Target breach also demonstrates that it's not enough to buy security systems. Firms need to keep abreast of potential threats rather than simply outsourcing and hoping for the best.

Target reportedly had invested in a sophisticated malware-detection system, but then neglected to respond to messages indicating the initial breach and taking appropriate technical steps to respond to the incursion.

Installing software or encryption technologies is not enough. Firms must ensure that the software is updated, fixed to appropriate settings (not necessarily "default" settings) and then monitored.

While law firms may not generally use their websites (or even mobile sites) to collect or transmit consumer data, firms are nonetheless fair game for hackers. In addition to retaining sensitive employee and client personal and financial information (for example, Social Security numbers and banking information), firms also may be targeted to access confidential client documents and communications.

It's not enough to simply delegate data security issues to third-party security/IT firms. Firms should adopt what the FTC has called a "culture of security." Firms should regularly train attorneys and staff on data security policies, but the broader lesson is to instill a sensitivity to potential threats, from leaving laptops unattended to opening suspect e-mails to downloading seemingly benign mobile apps on smartphones.

By creating a culture in which employees are constantly mindful of their online activities and report any potential breach or concern immediately, firms can prevent breaches — and take appropriate steps to mitigate any issues before they escalate into situations that would not only be potentially costly but damaging to client trust and goodwill.