DSnews

DEFAULT SE NT AND ONL SNEWS.COM » 01.2015

The View from the Bench:

LEGAL INDUSTRY UPDATE

Total coverage from top experts on the latest legal developments to hit the housing industry

PRESENTING THE 2015

BLACK BOOK

ANNUAL DIRECTORY OF DEFAULT SERVICING LAW FIRMS

NATIONAL

DATA BREACHES PUT SPOTLIGHT ON NPPI COMPLIANCE

By: Chris Hacker, ShortTrack LLC

Target. Staples. HomeDepot. These are just some of the most visible data breaches that happened in the U.S. this year. Over the same time, many real estate related operations, from title companies to lenders to attorneys, have increased their focus on making sure that the data they collect is safe from technological gaps and failures. And good thing—the coming implementation of the new CFPB disclosure rules in August 2015, and the increased regulatory scrutiny that comes with it, will touch all real estate professionals due to the CFPB's broad third-party service provider language. Unfortunately, that's also where many law firms and brokerages stop. Having a solid technological security approach and implementation alone does not stop those breaches. Sure, your servers are physically safe, and you've got firewalls and monitoring software protecting your data. You have reduced the odds of an unauthorized person or script from gaining access to your data directly, and that's important. But stopping here leaves the biggest security hole in your operation untouched.

The Real Security Weakness

From the earliest attempts at securing things with lock and key, the biggest security hole in every operation has always been its people and processes. Technology has come a long way in mitigating the risks posed by outside attacks and in managing internal ones; however, employees still have access to the data. And flawed, complex, or tedious processes inevitably lead to shortcuts that thwart the intended security of the process itself.

Take Non-Public Personal Information (NPPI), the most common data security concern in general and in real estate in particular. Typically, the response is "just encrypt the data," which is great while it's on your server. But, when you need to send a message or document containing NPPI, how do you keep the data secure during and after the sending? The answer has been to bolt-on one of three encrypted email approaches, sending an email to the recipient, let's call her Alice, with either A) a link to a Web portal where Alice must log in to view the specific data, B) an encrypted attachment, or C) full end-to-end email encryption (which is rare and hard to scale).

All three have technical requirements. Approach A requires Alice to either have or set up a unique login before being able to view the data. Approach B requires you to provide Alice with a password, which introduces security issues depending on how that's handled (especially when that password is emailed immediately before or after the attachment is sent). And Approach C requires Alice to have set up and made available a public and private key for use when you fire off the email (many who just read that did not understand it, which illustrates the problem I'm highlighting), plus once the email has arrived, it now sits unencrypted in Alice's inbox. And this last part is true no matter which approach is used—once the document is in the wild, it is out of your control.

Behavioral Resistance

However, the real issue is the behavioral requirements of the approaches, given their single-use nature. In reverse order, Approach C requires non-technically inclined people (Alice) to complete fairly technical acts to create and install email encryption keys and possibly software. Approach B requires you to take at least one extra step to contact Alice to provide her with the password, preferably by phone, which also requires Alice to be available at the time you call. Approach A requires Alice to visit an unfamiliar site, create a profile, and remember yet another password to log in.

In each case, there is behavioral resistance to meeting those requirements. Inevitably, Alice is a customer, either unwilling or unable to meet this requirement, and insists you 'just send it to me.' At that moment, you may have a written policy requiring you to use your encryption system, but you don't have an established process that actually supports that written policy. One of two things happens—you upset your client by denying her request to use an insecure channel (email), or you send the email and expose your organization to an NPPI breach.

Usable Process

The core of the problem just described is the implementation of a procedure that is not usable in the real world. The truth is the best written security procedures for protecting NPPI will still fall to human error. The challenge is to provide a process that both secures the data while not increasing the effort to collaborate. Rather than bolting-on one or more single-use systems, a collaborative software approach engages users throughout the process and in multiple ways, effectively keeping the user in the software by providing multiple valuable uses.

The key components of this approach are a robust and secure notification system, role-based transaction collaboration, secure document storage and sharing, and manual and auto encryption options. First, email isn't likely to go away for the foreseeable future, so you have to start with a notification system for all information. When NPPI is involved, the end user should have a password protected login. This is a significant upgrade over encryption Approaches B and C above. Second, a role-based transaction collaboration system helps secure personal information on the transaction with role-based invitations, and improves on Approach A-since Alice will know this login is not just for retrieving an occasional message, but for all matters related to the transaction. Third, the same role-based permissions should apply to document storage and sharing. Lastly, software with auto-encryption can recognize personal information, like a SSN, and stop it from leaving the system without an encryption protocol in place. Together, these components keep a user in the system by making it simple and easy to use.

The challenge is that much of what is still in use today is not ready for Web-based collaboration--it is on-premise, silohed, and designed to be isolated from the Internet. The knee jerk reaction to fix it with the duct tape of a separate encrypted email solution has been exposed above as a cumbersome and worked-around 'fix.' To stay compliant and ahead of the coming regulatory scrutiny, practitioners should implement software that have these four components, providing ready access to data while ensuring that data's ongoing security.