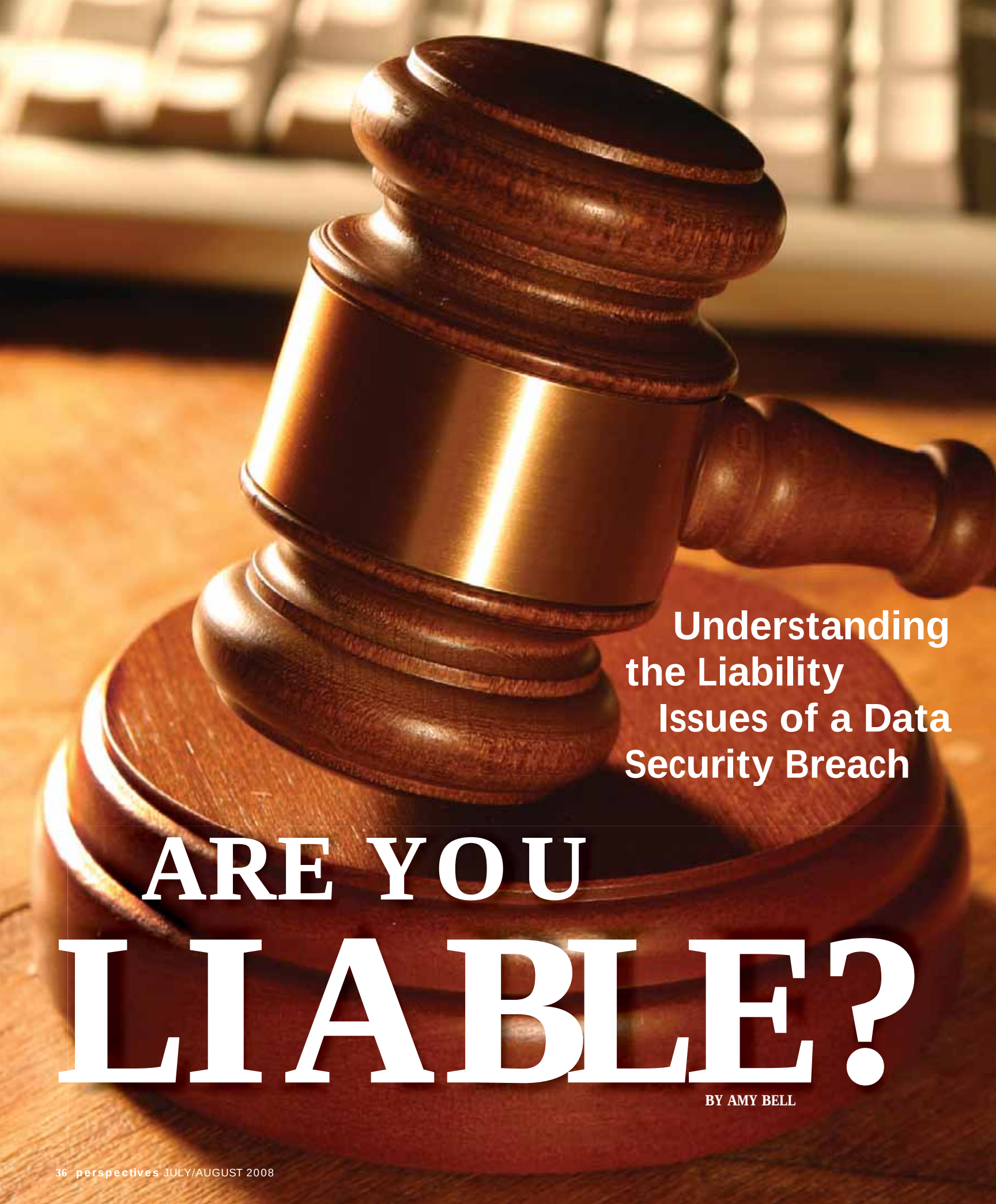


Understanding the Liability Issues of a Data Security Breach

ARE YOU LIABLE?

BY AMY BELL

"Data security breach": those three little words have the power to send shivers down any CEO's spine. The frightening phrase conjures up images of infuriated customers, bloodthirsty class action lawyers and hefty fines and settlement fees that could drain the life out of a business.

While no one enjoys thinking about the dreadful consequences of a data security breach, every BGA needs to understand and prepare for such a catastrophe, as the chance that many life insurance agencies will face a data security breach at some time or another are high. In today's electronic age, all it takes is one stolen laptop, lost PDA or a clever computer hacker who gains access to a company's records—and before you know it, your agency is spiraling into security breach chaos.

I recently spoke with Brian T. Casey, Co-Chair of the Insurance Practice Group with Locke Lord Bissell & Liddell, LLP, an Atlanta-based law firm that has worked on numerous data security breach cases. Casey helped to shed some light on the liability issues that can stem from a data security breach and offered some suggestions for how BGAs can work to prevent a breach from occurring in the first place.

Agencies can face a deluge of liability issues in the wake of a security breach, depending on the specific circumstances.

Understanding the law

First and foremost, it's vital that every BGA fully understands and abides by the privacy laws affecting their particular agency. All financial service companies fall under The Gramm-Leach-Bliley Act (GLB), also known as the Financial Services Modernization Act. This federal law requires that financial services companies have a customer privacy policy and notify customers of that policy each year.

But this is just one of many regulations financial institutions are required to follow. Oftentimes, the law an agency is expected to follow depends upon the state where the business and/or their clients reside.

"If you have 38 states that have data security breach laws, different flavors apply to each business whether it's a manufacturer or an insurance agency," Casey explains. "If you have a security breach, and you're subject to one of those laws, then you have certain obligations."

"For an insurance agency, under state implemented Gramm-Leach-Bliley privacy laws, there are requirements that the agency or any regulated entity, must follow," he says.

Under this law, he says, insurance agencies must have adequate procedural technical administrative safeguards and employ systems that are designed to deal with anticipated threats, such as hackers who could attempt to gain access to sensitive data.

"They need to have policy and procedures, and they need to have the technical safeguards—you know common sense things like passwords that expire every few months," he says. "There's also a physical element to it—they need to lock their filing cabinets and not leave data out in the dumpster. Basically there's a regulation—it's called safeguarding of consumer information—and they're supposed to be complying with that."

However, because the law varies depending on location and type of business, it's critical for every BGA to do their homework and understand the regulations they are required to follow.

A flood of liability issues

Unfortunately, even if a business follows information privacy laws to the letter, this does not guarantee that they will never suffer a breach. Probably the most terrifying aspect of a security breach for a business is the potential for endless legal nightmares. An agency could face a deluge of liability issues in the wake of a security breach, depending on the specific circumstances.

In the aftermath of a security breach, some businesses find themselves dealing with one legal headache after another. And many companies end up paying the price in a huge way—sometimes to the tune of millions of dollars.

"There's potential for civil liability outside of the security breach laws," Casey explains. "If there was negligence and a consumer was harmed, then they could sue for negligence under a civil lawsuit."

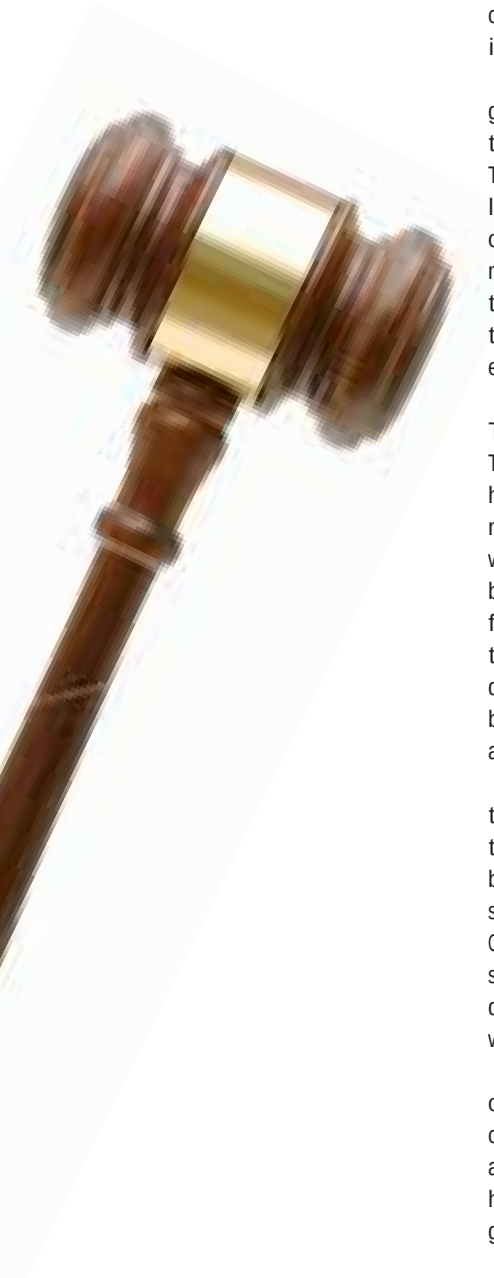
Not to mention that the BGA, and possibly their carriers, could face some lofty fines. "If the agency did not fulfill its requirements under these insurance regulations to maintain adequate safeguards, they could be fined. In theory, the carrier could be fined if the carrier wasn't policing its agents."

And just when you think things couldn't get worse, they can. "Under contract law between the agency and the carrier, there might be a breach of the contract by the agency, which would allow the carrier to terminate the contract or sue for damages if the carrier had liability," Casey says.

A real-life nightmare

ChoicePoint, an information broker, became intimately familiar with the many liability issues that go hand-in-hand with a data security breach. In this widely known case, ChoicePoint failed to confirm the identities of businesses requesting the data, as required by the Fair Credit Reporting Act (FCRA). Consequently, 163,000

Under contract law between the agency and the carrier, there might be a breach of the contract by the agency, which would allow the carrier to terminate the contract or sue for damages if the carrier had liability.



consumer records were compromised in 2005.

ChoicePoint had to shell out a grand total of $15 million to settle the massive security breach case. The company had to pay $10 million in civil penalties for violation of the FCRA and an additional $5 million for consumer redress. Additionally, ChoicePoint must submit to independent security audits every two years until 2026.

Taking action

The ChoicePoint case goes to show how important it is for every business to be prepared for the worst when it comes to data security breaches. That's why it's critical for every BGA to have a clear action plan in case a security breach does occur. "An action plan should be part of every agency's policies and procedures," Casey says.

While your security breach action plan should obviously include the steps you are obligated to take by law, you may also include some self-imposed measures, as well. Casey says the first step should simply be to determine if there has definitely been a breach and if so, what kind.

"I think the first key is to figure out whether you're subject to security breach law, and if so what are your requirements under that," he explains. "You've got to investigate to determine whether in fact there's been a breach and then figure out if you've got to comply with any of these laws. That depends on where the affected people reside and what type of security breach law is in play. And then you have to determine what potential harm is out there with respect to the type of breach, based on the nature of the information and who you think got it."

Depending on the laws you are required to follow, the next step in your plan may be to contact any clients who could be affected by the breach.

"Under security breach laws, some of them require notice to the affected persons," Casey says. "Some require that you, the person who was subject to the breach, notify the consumer reporting agencies so they can put a freeze on their credit report."

Even if you are not required by law to notify your clients after a breach, you may determine it is wise to do so anyway. "As a business practice, you need to consider whether or not you ought to notify the people from a customer relationship standpoint. I suppose you carry some risk, though, that you might spark a nasty plaintiff, but you've got to balance that versus customer good will. If it gets out there that you had one, that's pretty damaging to a company," Casey says.

"If you're going send notice to your customers if you don't have to, you need to consider that decision very carefully because it cuts both ways," Casey explains.

You may also need to notify your carrier of a potential breach. "If an agency has a breach, they're probably going to have to report it to the carrier regardless of security breach laws," Casey says. "That would be part of the protocol."

Of course, one of the final steps in your plan should be to repair the problem that led to the breach in the first place to ensure it doesn't happen again. "If it was technology issue by people leaving their computers on or wireless communications that were on access networks, those kinds of things, you need to fix that problem," Casey says.

"If [an agency] doesn't have written policies and procedures, that certainly ought to energize them to get that done," he says. "Once an agency incurs a breach, they have to look at the bigger picture and consider how to get in compliance with training and annual updates for their employees. And they also need to deal with it in their HR policies—people can get terminated if they don't adhere to the written policy regarding privacy and security."

Although the specific steps will be different for every agency, Casey stresses that every business should have some type of security breach action plan in place. "It's part of the whole risk management process—that's an important part of it," he says. "The protocol should be built into your overall policies and procedures for privacy and security."

In the end, an effective action plan could make a BGA's security breach nightmare a little less horrifying.