



**Swett & Crawford**

Everything We Know Goes Into Everything We Do™

## **Privacy and Security: Ignorance is not always bliss**

Author  
Mark A. Smith, CPCU, RPLU  
Swett & Crawford

There is no question about it. Most clients are unaware of their new liabilities under state and federal privacy laws. Unfortunately, unlike the old cliché, "ignorance is not always bliss".

In today's economy, even if clients are aware of their new liabilities, they are likely too stressed from trying to keep their doors open to be able to afford a premium for a new coverage they may not fully understand.

These facts present the typical retail agent a serious challenge. How do they educate their clients about their new liabilities, let alone explain and sell a new coverage most clients don't understand and really don't want to buy? Similar to the difficulty of selling Employment Practices Liability in the mid 1990's, it would be easy walk away, but the reality of these new exposures is too scary to ignore. In fact, doing so could lead to an agent's own E&O claim later down the road.

Like EPL, state and federal legislation is driving this train. Since 2003 over 45 states\* have enacted privacy laws applicable to any business or public entity. At the federal level, the HITECH Act went into effect this past February, and unless delayed again, the Red Flag Act becomes effective in June 2010.

All of this new legislation has very specific notification requirements if private confidential information is unintentionally released. Some laws even have enforcement teeth in the form of fines or penalties. Any client holding personal information from out of state customers must comply with any of the applicable 45 state laws, multiplying their potential for a regulatory violation and a potential fine.

Privacy breaches are simply defined as unintentional or accidental disclosure of personal confidential information. Most arise from lost or stolen laptops but may stem from errant emails, mislabeled mailings or an unintentional posting on a website or in a document. Security breaches often involve more sinister scenarios with potentially serious financial consequences for either the client or the client's customers. These often involve the failure of the client's security to

protect information secured in the client's computer system: a computer hacker stealing credit card numbers or a rogue employee selling off stolen social security numbers of customers to a crime ring for quick cash.

Third party liabilities from privacy or security breaches are expected to grow. For example, as medical files migrate to on-line systems, imagine the claim filed by a plastic surgeon's patient if the procedures were disclosed to the public by a hacker if an extortion demand is not paid! An increasing number of claims are filed by credit card companies directly against merchants who have suffered security breaches involving customers' credit card numbers. Contractual liability issues are also surfacing as many entities outsource much of their confidential data to third party vendors for accounting, data processing, billing, ecommerce or other services. A breach occurring while this information is in the possession of the vendor does not waive the regulatory requirements of the entity who entrusted it to them. Therefore, contractual transfers of these risks are increasing, especially with regards to health care entities in responding to the HITECH Act. Healthcare providers are inserting indemnification agreements into their "Business Associate Agreements" with their service providers (BA's) who work with patient's medical information on their behalf.

Another issue is liability arising from the disclosure of third party, confidential corporate information. Clients are more likely to be sued by corporate entities with whom they have signed a non-disclosure agreement if that information is later disclosed. Consider the unfortunate insurance agent whose laptop is stolen containing the latest financial statements of a financially distressed contractor unencrypted on the hard drive! That information, if made public, could potentially put that contractor out of business.

Standard insurance coverages do not provide the protection clients need to address their regulatory responsibilities and third party exposures. In response, over twenty insurance carriers now offer some form of both third party and first party protection. These policies, many introduced in the last year, include a highly complex array of insuring agreements, policy exclusions, endorsements and other options with no standardized coverage existing between carriers. First party coverages, which are direct losses clients may incur even in the absence of a third party suit, include notification and credit monitoring expenses, data restoration costs, crisis management, extortion and business interruption, all with various sublimits, deductibles or coverage triggers.

Agents need to take a deep breath and first familiarize themselves with the various privacy laws and the basic coverages available in the marketplace prior to addressing these issues with clients. Once these are understood, its time for posing a series of important questions in discussions with the client, assisting both the client and agent in understanding the client's true exposures. For starters, a few of these may include:

- Are you aware of the state and federal privacy laws and your notification requirements?
- Do you have any personal confidential client information stored on computers or in paper files on premises?
- Do customers use their credit cards to purchase goods on your website?
- Do you sign any confidentiality agreements regarding any information provided to you by others?
- Do you outsource any services to third party vendors which may involve a client's information?
- Do you sign any indemnification agreements with clients as respects their information they entrust to you?

Hopefully, after such a discussion, the client's eyes will be open to their true exposures. They may not be happy with these facts, but it's now in their court - either move forward and apply for coverage or ignore them at their own peril.

\*To view your state's law, go to:

<http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx>

© 2010 The Swett & Crawford Group, Inc.