Difficult Disclosure

>>BY CIP SOCIETY

In recent years, the industry has witnessed more than one incident involving compromised consumer data. Whether that breach was intentional—hackers breaking through firewalls and stealing data—or the result of human error, both situations beg the question: How do you protect information?

A solid data breach protection plan can prevent or mitigate situations that contravene privacy laws or threaten confidential information. Without one, the scenarios that follow can be costly, both from a financial and a reputational risk perspective.

SCENARIO 1: What if a well-meaning marketing representative, who was data-mining for a company pitch, backed up customer information on his laptop. He intended to clean up the data at home before a mail-merge, but before he had a chance his laptop was stolen.

SCENARIO 2: A well-meaning employee wanted to shred documentation that listed client credit card numbers. Rather than call a professional shredding company, the employee took the documents home to use his home shredder.

SCENARIO 3: An independent adjuster excelled at creating paperless workflow. He managed claims and investigations by e-mail and online while on the road. That is, until he mistakenly sent an e-mail containing reports and summations for one claimant to the wrong person.

SCENARIO 4: Many of us use memory sticks to transfer presentations and data. Have you ever left one behind after giving your presentations? Can you account for all the memory sticks you've ever had or used? If you can't, then you also cannot account for all the information they contain.

As insurance professionals, it is our personal and professional responsibility—and as insurance organizations, it is our legal and corporate responsibility—to ensure that all staff understand the issues, protections and protocols surrounding the collection, use or disclosure of personal information. As such, it is important we establish rules, install security and implement protocols to mitigate the risks of any type of data breach and preserve the integrity of our data.

If these efforts fail and there is a data breach, it is critical to assess the level of the breach and take action. This includes acting within an appropriate timeframe to re-establish control and to enable your clients to establish control; it also requires transparency—for a company, this requires that you notify all clients that their personal information may have been compromised.

Also, companies should suspend commercial activity and install more up-to-date firewalls, better encryptions, or other security protection. This action should also include direct calls to clients, where appropriate, or a mail campaign detailing the compromise to your data privacy. In the end, though, regular review and maintenance of data protection is the best defence. This should include regular business continuity assessments that will help your company take immediate action, if necessary, and will help your staff communicate both internally and externally to minimize the impact of a data breach, and to maintain the integrity of the data going forward. ■

The **CIP SOCIETY** represents more than 15,000 graduates of the Insurance Institute of Canada's Fellow Chartered Insurance Professional (FCIP) and Chartered Insurance Professional (CIP) Programs. As the professionals' division of the Institute, the Society offers continuing professional development, information services, networking opportunities, and recognition and promotion of the designations. This article is intended to generate a dialogue about ethics among professionals and we welcome comments and scenarios to the discussion at cips@insuranceinstitute.ca. This series of articles is archived on The CIP Society's website at: www.insuranceinstitute.ca/cipsociety.