

## **Inside 1to1 Privacy**

**Date: 04/23/2008**

**Issue: April 24, 2008**

**People: Don Peppers & Martha Rogers, Ph.D.**

### **Open Letter to the World: Don't Copy our Security-Breach Notification Model**

The U.S. experience with security-breach notification has been a huge success by several measures: Americans have been informed like never before about the status of their personal data, dollars have flowed into corporate privacy and security programs, and the overall risk to sensitive personal information in the U.S. has probably declined. But other countries considering a jump on the notification bandwagon-including Canada, Australia, New Zealand, South Africa, the UK and the EU-would do well to learn from our mistakes.

A December 2007 report summarizing seven chief security officers' views on the topic notes that one of the principal effects of breach-notification laws has been to raise executive-level awareness of data security and improve budget allocations to security programs. Entitled "Security Breach Notification Laws: Views from Chief Security Officers," and conducted by Chris Hoofnagle of the Samuelson Law School at the University of California-Berkeley, the study also pointed out some shortcomings and recommendations based on the U.S. experience since 2003.

With these findings in mind, we address this letter to the Privacy Commissioners in the countries considering adopting security-breach notification requirements in the near future.

#### **What would be our top three recommendations?**

Define a harm threshold for notification. The most prominent shortcoming of the American system is a tendency toward overnotification of supposedly affected individuals. "Overnotification" occurs when organizations feel obliged to inform customers and employees of incidents-such as misplaced backup tapes-that pose no material risk of harm to them. As noted in the Samuelson study, overnotification can result in unduly alarmed people as well as their disregard of subsequent notices. One solution to these unintended consequences is to define specific criteria when a data exposure risks harm to individuals, such as when there is positive evidence that an unauthorized person targeted their information for appropriation.

Provide guidelines for appropriate remedies. According to a study by the Ponemon Institute, in 2007 the average cost of a data breach in the U.S. was about \$200 per record exposed. Up to half of this cost is often to pay for credit-monitoring services for affected individuals. Even though U.S. state laws don't require this remedy, it has become a de facto industry standard, regardless of whether credit monitoring would do anything to help individuals affected by a breach. Credit monitoring, for example, would not help those whose medical data, e-mail addresses, or incomplete credit-card information was exposed. Providing guidelines that recommend remedies that fit the type of breach may help your country avoid this sometime misallocation of resources and false sense of security.

Define who is liable for costs related to a breach. The U.S. experience has shown that breach notification is costly, generating large bills for forensics and auditing, outside counsel, printing and call-center support, and the aforementioned credit-monitoring services. The bigger the breach, the more likely there will be a fight over who should pay for it. The victors in these fights are not always those who shouldn't pay for the breach, but can be those with the most legal resources. Your country can avoid our periodic misallocation of resources in this area by more clearly assigning cost responsibility to those whose errors caused the breach. The U.S. experience with security-breach notification hasn't been all bad, however. Your country could also take advantage of the two things that have gone well for us:

Define a short list of data fields of concern. What California did so well was to require notification for breaches of only those data fields that could be instrumental in harming someone through account fraud or identity theft. By limiting the scope of the law to a small set of identifying numbers, California and the states that followed it addressed people's main concerns, and made compliance more feasible.

Define an exemption for encrypted data. Although U.S. state laws lack needed specificity on this question, in practice, the near-unanimous exemption from breach notification is encrypted data. If a laptop is encrypted with industry-standard measures, for example, the risk of a laptop thief being able to get to the data is remote, and not worth alerting people. The Samuelson study goes further by recommending a broader safe harbor for other security measures that also may render information virtually inaccessible or unusable. The U.S. is widely reputed for having no central privacy commissioner, a patchwork of privacy laws, and an overall regime that fails the EU test of adequacy. That said, the U.S. has led the way in what could be the most effective type of privacy legislation the world has yet seen. Even if your version of security-breach notification is far from perfect, your country's citizens, and also its corporations, will be the better off for it.

You can reach Don Peppers and Martha Rogers at [dpeppers@1to1.com](mailto:dpeppers@1to1.com) or [rogers@1to1.com](mailto:rogers@1to1.com).