

THE JERUSALEM POST



Let my people know!

By DAVID MIRCHIN AND ANTHONY HERMAN

01/11/2012

Survey: 92% of data breach cases can be prevented by simple intermediate controls.

The recent disclosure of Israeli credit card details by a group of hackers is an opportune time to examine whether Israel should introduce data breach notification laws.

Such laws would require organizations to notify customers if their personal information is stolen or lost. This is important for two reasons. First, customers would be alerted about any theft or loss of their personal information and would then be able to take steps to protect themselves.

Second, notification laws would motivate companies to improve security measures to protect personal information they have collected from their customers because a failure to do so could result in a public relations nightmare and notification costs. As the old saying goes, “an ounce of prevention is worth a pound of cure.”

Similar laws already exist in other countries. California got the ball rolling in the United States 10 years ago when it enacted legislation requiring notice of security breaches. Most US states have followed that lead and now require organizations to notify the customers involved if they have been the subject of a data breach. Some states impose civil and even criminal penalties for a failure to properly notify.

The European Union is moving in a similar direction. The E-Privacy Directive already requires EU member states to introduce mandatory data breach notification obligations in connection with the telecommunications sector. Certain countries, such as Germany, have gone further and impose a more general obligation to issue notifications in cases of data breaches. Interestingly, the European Commission is currently proposing to fine organizations up to five percent of their annual turnover if they breach privacy regulations, which would be a meaningful incentive for companies to become even more serious about data protection.

Some organizations may argue that the cost for implementing security measures is too high. However, one survey shows that in 92% of data breach cases, simple intermediate controls could have detected and prevented the breach. There are now security experts who are saying that a standard and relatively inexpensive step like encryption could have foiled the Saudi perpetrators.

The cost for protecting customer data is not likely to be prohibitive and, in any event, should be less than the damaging effects of a data breach for an organization which may result in negative publicity and a loss of customer confidence.

Albert Einstein said that “in the middle of difficult lies opportunity.” While the Saudi hacker scheme is an unpleasant affair, it does present an opportunity for a public debate, and hopefully some legislative follow-up, about the need for data breach notification laws in Israel. The ideas bandied about in recent days, including the creation of an anticyber terror task force or a Bank of Israel investigation, would be helpful.

Like a modern-day Moses, we need a leader to stand-up and say: “Let my people know!”

The writers are lawyers in the Technology and Privacy Group at Meitar Liguornik Geva & Leshem Brandwein.

Copyright © 2014 Jpost Inc. All rights reserved •
[Terms of Use](#) • [Privacy Policy](#)