

A Data Security Mandate for Corporations, Non-Profits, and Government Entities

GUILLAUME DEYBACH

Companies must deal with data security issues — or face potentially significant liability.

The odds are that every corporate legal advisor, risk manager, or human resources professional (and every American, for that matter) knows someone who has had his or her identity stolen. With the issue of identity theft, especially for those who bear some level of corporate responsibility for privacy and data security, betting against these odds is clearly not prudent. When the breaches involve employee data, the stakes may seem even higher owing to the personal-professional connection to the victims and the fact that employee records tend to represent a large majority of reported data breaches.

Consequently, those who contribute to the development and execution of corporate privacy and data security programs are spending more and more time addressing employee data breach issues as the impact of such breaches — with their obvious links to identity theft — continues to grow in scope and significance. This trend toward tighter data security

Guillaume Deybach is the president and chief executive officer of Europ Assistance USA, part of the multinational Europ Assistance Group, which offers identity theft resolution services, travel assistance, emergency medical evacuation and repatriation, medical referrals, case monitoring, and international claims management.

reflects a clear mandate for corporations, along with non-profits and government agencies, to step up efforts to protect privacy.

The Federal Bureau of Investigation (“FBI”) said, “Identity theft has emerged as one of the dominant white collar crime problems of the 21st Century. Estimates vary regarding the true impact of the problem, but agreement exists that it is pervasive and growing.”¹ Other FBI estimates have placed the annual number of victims at up to 10 million with the annual cost to business topping \$50 billion.

In light of the scope of the problem, the litigious environment in the United States, and existing and emerging laws concerning corporate responsibility for the protection of personal data, corporate, non-profit, and government enterprises are being pressured to more actively protect the data of both employees and customers. The Better Business Bureau’s thoughtful actions to help small business owners fight identity theft by securing data demonstrate that this is not only a concern for large enterprises.² A closer look at the personal impact of identity theft reveals why it is a growing concern among corporate entities.

IDENTITY THEFT

In addition to the financial losses to individuals, the Identity Theft Resource Center (“ITRC”) said an average identity theft victim can spend hundreds of hours over the course of months or even years resolving issues related to a single theft.³ Because the customer service required to help consumers resolve identity theft issues is generally not offered on a 24/7 basis, victims often must take time during their workdays to resolve issues, creating a risk link between identity theft and employee productivity. Productivity losses, however, are not the only concern related to identity theft for companies.

Personal information can be stolen via the Internet when online transactions are made. Identity theft can also occur when there is some kind of personal connection between the thieves and their victims. For employers, a more critical concern is when identity theft can be tied to the action of employees, including both criminal theft of data by employees as well as the loss of computers or computer drives containing personal

data by employees. Employee actions — either purposeful or accidental — remain the largest single source of information breaches in both the government and commercial sectors according to the ITRC.⁴

THE VA INCIDENT

Perhaps the best known case involved the loss of up to 26 million personal records from the U.S. Department of Veterans Affairs due to an employee improperly taking the records home on a laptop computer, which was subsequently stolen. Other cases involved the U.S. Census Bureau, the National Oceanic and Atmospheric Administration (“NOAA”), Bank of America, Fidelity Investments, LexisNexis, and DSW Shoe Warehouse. The Privacy Rights Clearinghouse has chronicled the compromise of more than 200 million records of personal information in the United States alone. When employees mishandle personal data and losses occur, employers are culpable.

A Michigan case illustrates this culpability. In 2006, Michigan became the first state to require by law that every employer establish a policy for keeping employee Social Security numbers secure. The law was passed at nearly the same time a Michigan appeals court allowed victims of identity theft to recover financial damages from organizations that did not adequately protect personal data that were subsequently used for identity theft. In the court case, a labor union employee took home documents showing union members’ names and Social Security numbers; the employee’s daughter stole the information and used it to engage in identity theft. The union was found legally and financially liable for the actions of its employee.

In addition to the above events in Michigan, a number of other data protection initiatives have been keeping legislators busy in Washington and in state capitals around the nation.

CALIFORNIA’S RULE

California was the first state to pass a data security breach notification law. According to the National Conference of State Legislatures, to date no less than 39 American states have enacted such laws involving the

divulging of personal information. The federal government is considering statutes that go beyond breach notification to reducing the risk of breaches and providing harsh penalties for intentional acts of identity theft. U.S. government agencies, including the Federal Trade Commission, already have numerous privacy and data security initiatives in place.

All three branches of government, at the state and federal levels, are focused on identity theft, leading ultimately to increased statutory, regulatory, and legal pressure on corporations to protect personal data and protect their businesses from subsequent financial and productivity losses. In the private sector, the International Association of Privacy Professionals organized North American Data Privacy Day to focus attention on the importance of data protection, an event sponsored by universities, corporations, non-profits, and government agencies.

Common tools used by companies to ensure data protection include audits determining what employees have access to what data and why, stricter pre-employment background checks, document destruction policies and procedures, employee education programs, and more.

In addition, companies must manage productivity losses related to employees who themselves have become identity theft victims. Remember, as many as 10 million Americans are said to become identity theft victims every year — some 4 percent of the general population. But with current numbers of children, students, and retirees, 10 percent of the full-time workforce is probably a fair number.

Assume an employee strives to minimize work time spent on such matters, keeping it to just two hours per week for a total of 100 hours (a conservative number). Against a 40-hour week and across a 50-week year (allowing for two weeks of vacation), this represents a 5 percent productivity loss per affected employee with the very real possibility of 1 in 10 employees being affected.

SIGNIFICANT COSTS

The potential costs of these productivity losses can be staggering, especially when considered along with related regulatory compliance

costs and potential legal liabilities. A 2006 study put the average corporate cost of remedying a personal data breach at \$182 per breached record.⁵ When a company's data security program is to blame for the loss of productivity, the impact can be multiplied. The profound personal impact on victims adds considerable pain and suffering to the time and financial losses. Stemming such losses can easily become at once a philosophical, professional, and personal undertaking.

Over the past few years, the risk management industry has developed insurance products that assist corporations in minimizing certain losses related to identity theft. One comprehensive product from Europ Assistance USA is its Data Breach Response Service. The service helps corporations protect themselves, their customers, and their employees from the negative impact of breached data and identity theft. If a breach occurs, affected customers and/or employees can be notified in a timely manner through the service. The related ID Theft Resolution Services, often added to a company's package of employee benefits, helps victims quickly and easily recover from identity theft. The services include assignment of a specially trained coordinator who personally assists the victim by doing the necessary paperwork, making appropriate phone calls, and completing other restoration activities, such as credit report reviews, account cancellations, disputed items removal, and more, on behalf of the victim. The work is done by a specialist trained for such cases, and the employee is freed up to focus on work instead of restoring his or her good name. Such products enable employers to become part of the solution in addition to actively fighting the problem.

POLICIES, SYSTEMS, AND PROCEDURES

Many of the corporate risks associated with identity theft can be mitigated by the development and implementation of sound policies, systems, and procedures. Others will ultimately become matters for the courts. Risks that flow from the affected individual, however, must be managed using available tools and products that both support the individual and protect the employer — especially when the victim is an employee/co-worker. In the absence of a solid corporate privacy and data

security strategy, the potential losses due to the spread of identity theft are nearly unlimited. Choosing not to actively deal with the issue of corporate data security is tantamount to betting the company's future against significant odds.

NOTES

¹ *Financial Crimes Report to the Public*, May 2005, U.S. Department of Justice, Federal Bureau of Investigation.

² *Security and Privacy — Made Simpler*, ID Theft & Fraud Prevention Initiative of the Better Business Bureau.

³ In its "Facts and Statistics" published at http://www.idtheftcenter.org/art-man2/publish/m_facts/Facts_and_Statistics.shtml, the Identity Theft Resource Center cited recent average times spent rectifying ID theft-related issues as 330 hours in 2004 and 600 hours in 2003. In 2006, averages dropped to 97 hours for the simplest of cases, 231 hours where a new account was created, and escalating numbers of hours according to the severity of the theft.

⁴ This information also cited in ITRC's "Facts and Statistics."

⁵ Larry Ponemon, Ponemon Data Breach Study, Oct. 2006.