

## Five Steps for Managing the Risks Associated with Sensitive Data

By **Jonathan M. Cohen**  
and **Elise Dieterich**

In the “Information Age,” data has become a form of currency, and the types and quantity of data that businesses collect, store, buy, sell, and manage continue to expand. Sensitive, personally identifiable information (“PII”) such as names, Social Security Numbers, account numbers, dates of birth, and physical and virtual addresses are collected and used for virtually every corporate function: human resources, marketing, sales, customer support, technical support, product development, investor relations, regulatory compliance — the list goes on. Companies also handle sensitive data related to intellectual property and trade secrets that must be protected.

Industries like banking and health care that are subject to specific privacy and data security laws have long been sensitive to the risks and potential liabilities associated with handling PII. But, many other businesses are just beginning to become aware of the re-

---

**Jonathan M. Cohen**, a member of this Newsletter’s Board of Editors, is a partner at Gilbert LLP, which frequently represents policyholders in recovering insurance and other assets. He can be reached at [cohenj@gotofirm.com](mailto:cohenj@gotofirm.com). **Elise Dieterich** leads the Privacy & Data Security practice group at Sullivan & Worcester, LLP. She can be reached at [edieterich@sandw.com](mailto:edieterich@sandw.com).

sponsibilities and exposures that come with handling employees’ customers’ and other people’s data. The trend toward cloud computing, use of third-party application service providers, and outsourcing functions that can include payroll, benefits, marketing and more, multiply the potential vulnerabilities, and up the ante when it comes to managing data-related risk.

### RECENT CASES

Recent, high-profile cases illustrate all too vividly the financial, legal, and reputational damage that can occur when sensitive data goes astray. For example, a 2008 data breach that exposed roughly 130,000 customers’ credit card numbers is still dogging the dining and entertainment chain Dave & Buster’s, which in March entered into a settlement with the Federal Trade Commission (“FTC”) that requires the company to create a program aimed at protecting customer privacy and preventing another data breach, and to undergo an audit every other year for the next decade to ensure it is meeting the terms of the settlement. Similarly, CVS Caremark last year agreed to settle with the FTC, and its pharmacy chain agreed to pay a \$2.25 million fine, in connection with reports that its pharmacies around the country were disposing of sensitive information, including prescriptions and credit card numbers, in open trash containers.

As these examples show, companies that release PII, whether accidentally

or otherwise, potentially face at least two types of claims: those by the individuals whose sensitive information has been exposed, and indemnification or damages claims by credit card issuers or other companies that may have incurred losses as a result of the breach. The Identity Theft Resource Center’s 2009 Breach Report, released this January, lists 498 data breaches that exposed an estimated 222 million records. The Ponemon Institute’s recently published “2009 Annual Study: Global Cost of a Data Breach” found that the average cost of a data breach in the U.S. was \$204 per compromised record, a figure higher than other countries studied. Multiplying that figure by the 222 million records thought to have been breached last year yields a staggering cost to U.S. businesses.

Because the risks are high, companies should focus on putting into place procedures to minimize the likelihood of a release of sensitive information and to mitigate the damage if a release nonetheless occurs. In this article, we identify five steps every business should take to ensure that it is facing and appropriately managing data-related risks. In this area, more than most, an ounce of prevention can truly be worth a pound of cure.

### 1. KNOW WHAT YOU’VE GOT

Among the first steps every company should take in evaluating its information security is to catalog every place where the organization acquires, uses or stores potentially sensitive data.

Common data portals include the company Web site (are there contact, registration, or application forms online?); the employment process; and information collected for marketing and sales purposes. Find out who is in charge of each type of information, and who has access to it. Is information shared with outside vendors or other third parties? Determine what physical and technological safeguards are in place to protect sensitive data. Make plans to stop collecting and destroy PII that the company doesn't actually need.

## **2. KNOW YOUR OBLIGATIONS**

To protect employees and consumers, a host of federal and state authorities have implemented an alphabet soup of privacy and data security laws. Depending on the kinds of data your company handles, acts with acronyms such as CAN-SPAM, COPPA, ECPA, FACTA, FCRA, GLBA, or the USA Patriot Act may apply. Private standards, such as the mandatory Payment Card Industry Data Security Standards or Direct Marketing Association voluntary rules, may also be applicable by contract. And, of course, both the Federal Trade Commission and state attorneys general have become increasingly aggressive in their enforcement of laws prohibiting "unfair and deceptive trade practices" against companies that say one thing about how they will use information they collect, then do another.

In the event of a breach affecting PII, 41 states and the District of Columbia impose requirements — all different — regarding notification to law enforcement, regulatory authorities, and individuals whose information may have been compromised. The FTC's "Red Flags Rule" requires many kinds of businesses to have in place identity theft prevention plans, and special federal rules have recently been enacted governing breaches affecting health-care information protected under HIPAA. Several states have implemented laws requiring proactive data

protection measures, with more surely to follow. Canada, the European Union, and many other foreign countries have data protection laws that may apply to information gathered from their residents and stored on U.S. companies' servers.

Be aware, also, that it is increasingly common for the government to request information about individuals from companies that have such information in their possession — and not every government request is valid, particularly if the request is not supported by a proper subpoena. Any request to release PII should be carefully vetted, as the phone companies very publicly learned when they cooperated with government requests for customer information in the post-9/11 period.

## **3. KNOW YOUR PARTNERS**

If your company handles sensitive data for others, or relies on outside vendors for functions that require the company to share its data, it is crucial to know exactly how each and every vendor agreement addresses privacy, confidentiality, data protection, and responsibility in the event of a breach.

Assigning data-related risk contractually is one of the most important risk management strategies — but to do so, the company has to know what is already in its agreements. Evaluate whether your vendors can make good on their data protection promises. Particularly if your company is entrusting an outside vendor with PII, consider what due diligence is appropriate to establish, should there be a future breach, that the company was not negligent in relying on the vendor. Likewise, consider whether the company's own internal policies and procedures are adequate to answer potential third-party complaints. Companies should: 1) obtain and confirm representations and warranties attesting to each vendor's data protection capabilities; 2) put into place covenants to protect sensitive information; 3) require indemnities

and, if the vendor lacks deep pockets, insurance, bonds, or other security in case the worst occurs; and 4) consider carefully whether indemnities that it obtains have an adequate scope and are sufficiently reliable to provide the needed protection.

## **4. KNOW WHETHER YOU'RE COVERED**

Faced with a data breach that potentially could result in disclosures of private information, companies may look to their insurance policies for protection from resulting claims, costs, and liabilities. As a result, before a data breach occurs, companies should take aggressive steps to ensure that they have the coverage that they need. In particular, companies should conduct an audit of their insurance portfolios to identify potential gaps.

Some companies have obtained specialty insurance policies, sometimes called cyber-security insurance policies, that are designed specifically to address data-breach and cyber-security claims and losses. These policies may include both third-party (cyber-liability) and first-party (cyber-crime expense) coverages. These policies' third-party coverage can protect against claims ranging from lawsuits for unauthorized access to or dissemination of the plaintiff's private information, intellectual property and trademark and copyright infringement, or reputational injury including invasion of privacy, to conduit injury claims, including suits due to system security failures that result in harm to third-party systems, and injuries to customers arising from impaired access to an insured's system. Cyber-security insurance policies' first-party coverage often protects against costs such as privacy-breach notification expenses, crisis management costs, and e-business interruption.

Perhaps because cyber-security insurance policies are relatively new to the marketplace, and in some cases may be cost-prohibitive, many

companies do not have such policies in their current coverage portfolio. These companies nonetheless may already have insurance policies that potentially apply to claims and losses that might arise from a data breach. For example, general liability insurance policies may require the insurer to cover third-party claims for injuries arising out of the publication of material that violates a person's right of privacy. Although this coverage is phrased in terms of "publication," courts have held that merely inadvertently making private information available to the public, even absent actual disclosure, may be sufficient to satisfy the publication requirement and trigger coverage.

In many cases, insurers will raise defenses to coverage for data losses. It is important for policyholders to understand ahead of time the arguments that can be made on their behalf. For instance, although insurers may argue that a data breach falls under the standard-form exclusion for "knowing" violations of another's rights, policyholders often can respond that the breach was the result of negligence, theft, or other wrongdoing outside of the policyholder's control. As a result, it can be argued that the policyholder did not have advance knowledge that would trigger the exclusion's application.

Depending on the type of claim or loss, other types of policies also might apply. If a company incurs a business interruption because of a data-breach, that company may find coverage under its first-party property policy or a separate business interruption policy. If the data breach allegedly results from professional error or negligence, a company might have coverage under its Errors & Omissions policy. If a data breach results in securities claims or claims against a company's directors or officers, many companies have coverage to protect against such claims. Even a company's crime and fi-

delity policies might provide a source of insurance coverage, particularly if that policy contains an endorsement for computer-related crimes.

By reviewing coverages before an adverse event occurs, companies can best protect themselves for that eventuality.

## 5. HAVE A PLAN

Armed with the information described in tips 1 through 4, you are ready to formulate a comprehensive, company-wide data-related risk management plan. Actually, two plans: First, an ongoing plan to govern how data is collected, handled, stored, shared, and accessed day-to-day. And, second, a plan to govern how the company will respond if the worst occurs and, despite best efforts, sensitive data is lost or stolen.

The first plan will include external privacy and confidentiality policies, and internal policies to ensure data protection. Questions of who will have access to sensitive data, and what physical and technological safeguards will be imposed, must be addressed, usually in the form of IT policies and procedures, but be sure to address paper records, as well. Employee handbooks and training should be updated to reflect the company's data protection best practices. Vendor contracts should be updated to incorporate clear and consistent terms addressing responsibility for data protection, and due diligence should be conducted as needed.

The plan should include a comprehensive review of the company's insurance portfolio, and any prudent additions to coverages. Rules for employee use of company networks and, in particular, social media such as Facebook and Twitter, should be clearly articulated. Internal responsibility for compliance with all applicable state and federal laws should be assigned to appropriate supervisory and managerial employees.

Second, the company should put into place a plan to detect and respond to any unauthorized access to, possible loss, or breach of sensitive data. This plan should address who is responsible in the first instance for being on the lookout for data incidents, including computer hacking; loss of physical files, devices or drives containing sensitive data; and misuse of data by company employees or vendors. The plan also should spell out how, once a breach is detected, the company will respond, from an IT, legal, insurance, and public relations perspective. In particular, the plan should include putting into place a pre-arranged group of people from both inside and outside of the company who, collectively, can address all of the potential contingencies that a data breach might create. The plan should address who will determine whether the breach is reportable under various federal and state laws and, if it is reportable, how the reporting and other response requirements will be carried out. Responsibility should also be assigned for assessing the availability of insurance coverage, notifying the company's insurers, and keeping the insurers informed to the extent required by the insurance policies.

## CONCLUSION

While the parameters of businesses' responsibility for data protection remain uncertain and in flux, it is crystal clear that the costs and liabilities associated with failing adequately to protect sensitive data, particularly employee and customer PII, are on the rise. By following the five risk management steps outlined above, companies can help reduce the risk of adverse data incidents, and position themselves to mitigate the damage if an incident occurs.