*Creating a*
***culture of security***
*is key to stopping*
*a data breach.*

By Robert A. Listerman, CPA, CITRMS, and
James Romesberg, CITRMS

# ARE WE SAFE YET?

Identity theft and breaches of a company's data are rampant. According to the Identity Theft Resource Center, the rate of data breach incidents has risen more than 400% since 2005 when they started tracking such information. Since then, more than 245 million personally identifiable records have been breached from hacker intrusions to careless handling of sensitive information. And that's not all. The Center noted there was a total of 656 reported breaches at the end of 2008, which reflected an increase of 47% over the 2007 total of 446. For a breakdown of types of breaches, see Table 1.

### Table 1: 2008 DATA BREACHES BY CATEGORY OF SOURCE

| Category | # Incidents | # Records Lost |
|---|---|---|
| Financial Institution | 78 | 18,731,947 |
| Business | 240 | 5,886,960 |
| Educational | 131 | 806,142 |
| Gov/Military | 110 | 2,954,373 |
| Medical/Healthcare | 97 | 7,311,833 |
| **Total** | **656** | **35,691,255** |

*Source: Identity Theft Resource Center*

This epidemic rise in data breaches is why the U.S. federal government wants every organization to take measures to secure the sensitive data they maintain. So far, 44 states, the District of Columbia, Puerto Rico, and the Virgin Islands have implemented specific laws requiring enterprises that lose personally identifiable data to report the incident to individuals and provide a mitigating response. Perhaps you've even received one of those "Oops" letters stating that "your information was compromised…" The states that don't have security breach laws are Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota.

Federal laws that address organizations' responsibilities to safeguard sensitive information include:

- Fair and Accurate Credit Transactions Act (FACTA),
- Gramm-Leach-Bliley Act (GLB),
- Health Insurance Portability and Accountability Act (HIPAA), and
- Federal Educational Rights and Privacy Act (FERPA).

All these legislative acts impose penalties and open the door for civil liability if you've mishandled sensitive data. Size of enterprise isn't an excuse, so even a self-employed individual isn't exempt. (We aren't attorneys, so please consult with yours to understand which laws apply to you and your organization.)

Customers also might react negatively. According to the article "The Coming Pandemic" by Michael Freidenberg in the May 15, 2006, issue of *CIO* magazine, a technology industry trade journal, "If you experience a data breach, 20% of your affected customer base will no longer do business with you, 40% will consider ending the relationship, and 5% will be hiring lawyers!"

By implementing what we call a *Culture of Security*, your organization can greatly reduce the possibility of an embarrassing and costly data breach.

Here's an analogy. Bob attended a church retreat weekend a few years ago. As attendees moved from the main program area into small group rooms, they left recent purchases in the main room. Some women even left their purses behind. People finished their small group assignments at different times, so they wandered in and around freely until the main program resumed. There wasn't one incident of lost or stolen items. Would you do the same at a professional football game? Of course not, because the cultures of the two events are quite different. In a culture of honesty and a high degree of trust, where people are bonded together under a common cause, even open temptation is mitigated by a culture of security.

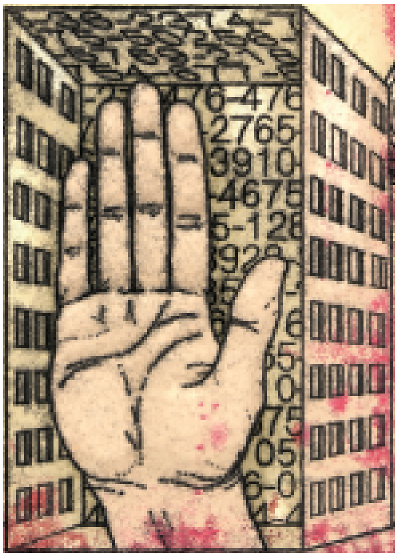
## Lay the Foundation

You may think that creating a culture of security is a major undertaking, but, by following a few simple, low-cost steps, it isn't as difficult as you may believe.

### Identity Theft Awareness and Protection Seminar

Start the process by involving all employees in an identity theft awareness and protection seminar that's designed to heighten their knowledge of the many problems a person may encounter when his or her identity is stolen. Here's a content outline of an effective seminar:

**A.** Use factual data from the Identity Theft Resource Center on the number of data breaches from 2005 to date. The information includes which organizations breached the data. Once employees understand the magnitude of the data breach problem, including the possibility that their own data is at risk, they start to understand



*It takes an identity theft victim an average of* ***58 to 231 hours of personal time*** *to deal with all of the record correcting and legal issues.*

why federal and state laws have been enacted to hold enterprises both civilly and criminally responsible for mishandling personally identifying information (PII).

What is PII? The obvious list includes social security numbers, driver's license numbers, and financial account numbers such as credit card numbers. But any information that would allow a person to assume someone else's identity is what a thief needs. Personal nonpublic information such as birthdays, mother's maiden name, pet names, passwords, home alarm codes, wedding anniversaries, and any other unpublished or unlisted information can be considered PII.

**B.** Add video interviews of people who have had their identity stolen. You can find all that you'll need on the Internet from sites like YouTube. Be sure to include at least one for each type of identity theft so employees realize that it may involve more than financial theft. You can show victims of medical, criminal, and character identity theft as well as financial. The gut-wrenching stories of these innocent victims, who make it clear that this could happen to anyone, bring home a message that nobody wants to experience a life-changing identity theft incident.

**C.** Teach employees what they can do to detect if an identity theft incident has happened to them. Cover how FACTA gives them the right to request a free annual report from businesses that collect data on them for resale, such as credit bureaus. They will learn that monitoring the data reported on them is a way to view if misinformation, including activities from an identity thief, is added to their file.

The seminar brings everyone to the same understanding of the problem. Once all employees have learned the importance of the problem, their acceptance of and full participation in your organization's program to prevent a data breach become more plausible.

### Tone at the Top

People react to what you do, not to what you say. The behavior of top executives instills culture. Even the Federal Trade Commission (FTC) recognizes this because it wants your data security program to be formally implemented by the board of directors or, if no board, the owner or CEO. We suggest that you take the FTC's fine suggestions and then leverage how to actually change the culture.

Start by helping your employees with their own identity theft risks. When an employee suffers an egregious incident of identity theft, it will negatively affect his or her attentiveness (and productivity) at work. According to the Identity Theft Resource Center, it takes an identity theft victim an average of 58 to 231 hours of personal time to deal with all of the record correcting and legal issues. The Center further reports that it may cost an individual thousands of dollars in out-of-pocket expenses, including attorney fees.

## Protect Your Own Employees

To accomplish this, we highly recommend you kick off the implementation of your culture of security by offering your employees an employee benefit of an identity theft protection service that will handle all the restoration and legal issues of an identity theft incident. This not only helps them, but it also helps your organization in several ways:

◆ First, knowing that an experienced professional is handling their case will help keep employees productive.

◆ Second, having all of your employees under the same service provider umbrella may act as an early-warning signal that something is wrong internally if a statistically abnormal number of your employees experience identity theft issues at or near the same time. Early realization of the existence of an internal breach will mitigate any damages to your organization.

◆ Third, it demonstrates how strongly your organization feels about implementing a culture of security. Nothing is more demonstrative in making a culture change with employees than putting them first.

We know many organizations are struggling with increasing costs of employee benefits, especially healthcare. But the cost of an identity theft protection program can be kept to under $30 a month for the entire family. If you can't afford $30 per employee, then consider offering it as a partially subsidized fringe benefit to offset the cost. Remember, though, you want a high level of participation to act as a possible early warning that something may be wrong internally.

## Form a Data Security Project Team

To continue the implementation of your culture of security, have your employees make this project their own. Letting them actively participate in helping the organization protect the personally identifying information you must manage gives them ownership in the solution. Ownership in the solution lessens any resistance to changes they need to make to reach data security goals.

To form a data security project team, top management needs to appoint a data security officer (DSO) who's capable of understanding the entire operations of the enterprise. This person needs to be part of senior management. Some of the usual designees are chief financial officers (CFOs), HR directors, and, of course, chief information officers (CIOs). All are acceptable, but remember that this isn't just about technology. (Our technology friends enjoy it when someone realizes that data security isn't all their responsibility.)

We recommend that the data security officer include representatives from all departments on the data security project team. The importance of this will become evident when we review specific procedures.

## Follow the FTC Guidelines

The following steps have been adapted from the Federal Trade Commission's brochure titled *Protecting Personal Information: A Guide for Business*. We also adapted the FTC guidelines and website information into our *Protecting Personally Identifiable Information in the Workplace: A Study Guide*. Our study guide's step-by-step procedures document what a company needs to do and has done to implement reasonable measures to prevent data breaches.

### Inventory Sensitive Data

The first step from the FTC guidelines is to "Take Stock," or inventory what data you collect and maintain. Have *all* employees list every document they touch throughout the day, week, month, or whatever cycle time frames the data security project team decides. Have them identify the document by name, what PII is on the document, and how they receive the document into their area. Then take that same procedure and apply it to electronic documentation on the computer screens they access.

By having all, and we do mean *all*, your employees perform this exercise, they become truly involved in the overall culture of security implementation. Having this input come back to the data security project team helps minimize the team's workload and also helps make sure all data types and locations are inventoried. Don't overlook data storage devices, such as flash drives, disks, home computers, or any other equipment. Your inventory isn't complete until everyone has checked every place sensitive data might be (or has been) stored.

### Scale Down the Data You Keep

The next FTC step is to "Scale Down."

The first opportunity to scale down is to determine what sensitive data you're collecting or maintaining that you really don't need to collect. One simple example is social security numbers on job applications. Since you don't need anyone's number until you hire, don't ask for it. By doing this simple procedure you've reduced the impact on the entire applicants' data file should it be compromised. Each time you apply this thought pattern to the collection of sensitive data, you are scaling down and mitigating the consequences of a data breach on that data type.

The next opportunity to scale down comes from reviewing collection points and timing. Perhaps there are collection points that are more vulnerable than others, such as files kept in a reception area or other general access area, and simple process changes can greatly reduce the likelihood of a data breach. Look for process changes that will get the sensitive information into its secure permanent storage the fastest. For example, don't allow any sensitive data to lie in an unsecured "holding bin" overnight.

*You'll know when your **culture of security** is in force when you hear or see employees conduct themselves in a manner that says they are "looking out for each others' backs."*

Tell all employees that their assistance will be solicited and that they should feel free to volunteer their ideas when they see any opportunity to improve the handling of sensitive information. Also tell them that they should never take it personally or feel like they've been demoted if, as a result of this program, their access to information is reduced or eliminated.

Another scaling-down technique is to give all collected data a "life span" for disposal or deletion. Knowing how long data needs to be kept and getting rid of it safely (more on how later) will reduce your exposure if the file is compromised. Eventually you'll be writing an organization-wide *Sensitive Information Policy and Program*. Part of this program will be your records-retention policy.

### Physically Secure Sensitive Data

The next FTC step is to "Lock It."

Physical security starts with your premises. All areas, rooms, closets, cabinets, files, desks, and waste containers have to be reviewed. As we mentioned earlier, the *temporary* physical security, where sensitive data flows through all of your organization, also must be included. Limited access to certain areas where sensitive data flows and is stored is also a "physical" security issue. The data security project team needs to walk the sensitive data pathway and evaluate whether the physical security—temporary and permanent—is appropriate.

Physical security is probably the component of your overall data security plan that's most positively affected by the implementation of a culture of security. You'll know when your culture of security is in force when you hear or see employees conduct themselves in a manner that says they are "looking out for each others' backs." For example, you may hear one employee remind another to place a document into a secure location before leaving for lunch. Your culture of security gives that employee the right to remind the other employee.

Locked doors, cabinets, and desk drawers are still the best way to minimize exposure to individuals who don't have a "need to know" the information. We suggest that you implement a "clean desk" policy for documents containing sensitive information as part of your physical security policy.

Paper documents aren't the only items that need physical storage protection. CDs, DVDs, and any electronic storage devices containing PII need to be physically secured. Follow the FTC's guidelines in this area, and make sure you have your IT department or technology consultants on your data security project team.

### Dispose of Sensitive Data Properly

The next step is to "Pitch It." It never ceases to amaze us how otherwise sophisticated organizations will do dumb things with their "trash." Your trash may be an identity thief's treasure.

Your PII policy and program need to address the proper disposal of each sensitive data type inventoried in the first step. The disposal doesn't have to be an expensive part of your data security program. Here are some simple suggestions:

**A.** Have cross cut shredder(s) easily accessible in departments that handle sensitive physical documents. Place a shredder near your photocopier for easy disposal of PII, and place one near the desks of employees who handle sensitive information.

**B.** When you dispose of electronic devices, make sure you use a "wipe" utility program or physically destroy their data storage components.

**C.** Make sure remote users, including those who work from home, follow the same written disposal policy you practice in the office.

**D.** For high-volume, sensitive-document handling, consider having a qualified shredding service manage document destruction. They will place secured "bins" in appropriate areas throughout your organization to make it easy on your staff to comply with your PII disposal policy and program.

### To Avoid Panic, Plan

The next step in the FTC's guidelines is to "Plan Ahead."

Despite all your efforts, a breach can still happen. But there are ways you can greatly reduce the negative impact a data breach can have on your organization and on those who trusted you to protect their personally identifying information.

Have a plan in place to respond to any security incident. Know what you would do based on each data type you maintain. Your data security officer must know the proper response as soon as the incident occurs.

There are a couple of things to consider. That *CIO* article we mentioned previously also stated that "a data breach incident costs an organization about 1,600 hours to clean up and $40,000–$92,000 per identity theft victim." Most organizations go into panic mode when they discover they have a data breach incident to manage. In panic mode you run the risk of either underreacting or overreacting to the incident. If you underreact, you expose yourself to less sympathy, which could lead to greater awards a victim may receive as the outcome of a lawsuit. If you overreact, then you're spending more time and money than necessary to mitigate the effect of a breach. When you're in panic mode, you also are more likely to make additional costly mistakes.

We recommend that larger companies engage a public relations firm in the planning process who will map out how to handle the breach announcements to law enforcement, the victims, and the public at large. Having the PR firm involved in the planning process means you both know ahead of time what to do and can immediately be ready to deploy your plan.

## Your Sensitive Information Policy and Program

You are now ready to start putting together your formal *Sensitive Information Policy and Program*, which delineates in writing the policies and procedures for keeping your sensitive information safe and describes what to do if you have a data breach. When we consult with an organization, we provide a sample template they can tailor to their own needs. But you can do an Internet search for "Sample Sensitive Information Policies" and find ones for purchase that are easy to use on your own.

*Most organizations go into **panic mode** when they discover they have a data breach incident to manage.*

If a company has "covered accounts" with its customers, we include a "Red Flags Rules" section in the template. This information stems from the FTC's publication, *Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003*. The pertinent part for this article reads: "Under the final rules, only those financial institutions and creditors that offer or maintain 'covered accounts' **must develop and implement a written Program**. A covered account is (1) an account primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions, or (2) ***any other account*** **for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft**. Each financial institution and creditor must periodically determine whether it offers or maintains a 'covered account'." (emphasis added)

To make a template your own, the data security project team needs to make changes based on your operations. Department heads should read through draft versions of the tailored document. Have discussions with them regarding how the proposed policy and program may affect process flows or procedures once they are implemented. Let the department heads offer their suggestions. Once the department heads and the data security project team have hammered out any changes to support the organization's new *Sensitive Information Policy and Program*, bring it before top management and the board of directors for their review and final approval.

## Employee Training

Mandatory employee training can begin with the rollout of your new *Sensitive Information Policy and Program.* Go through the entire document with each group of employees. Perhaps they will offer more good ideas when they get their arms around this new policy and program. Since you involved them from the start by educating them about the importance of protecting personally identifying information when they attended the Identity Theft Awareness and Protection seminar, offered to help protect them personally, and had them help inventory the PII data they work with, you will have people who are very willing to make your new program work. Your goal is to make this policy and program theirs.

Explain their roles and that you need their help in spotting security vulnerabilities. Make this training part of new employee orientation. Ongoing periodic training emphasizes the importance you place on meaningful security practices, so plan to reconvene the group after a period of time to get their input as to how the program is working. A well-trained workforce who has made protecting sensitive data their responsibility is the best defense against data breaches.

Have all employees sign a document that states they have attended the training and have been instructed on their responsibility in the use of confidential information. Again, we have templates that can easily be made yours. Send us an e-mail, and we will provide ours at no charge or obligation.

The FTC recommends that you check references and do background checks before hiring new employees who will have access to sensitive information. We recommend that you do background checks on *all* new hires, regardless of their position or handling of sensitive information. If they want to steal information, they will learn how to get access to it once they are inside your organization.

In areas where sensitive information is used or stored, as well as where employees congregate, post reminders of your polices on keeping information secure and confidential. Make sure these policies cover employees who telecommute from home or an offsite location.

## Your New Culture of Security

Congratulations on installing a culture of security. How do you know for sure? The culture was changed when you completed the program we just described because you gave your employees what they need to comply with your new culture of security.

We know this because you brought everyone through a journey that started with the sincerity demonstrated by the owners themselves. You brought everyone to the same level of awareness through the Identity Theft Awareness and Protection seminar and the immediate identity theft protection service you offered each employee. Then you had your employees take ownership of what we like to call a sensitive "data hygiene" process, including inventorying, scaling back, physically and electronically securing, and disposing of sensitive information appropriately.

You made changes based on the discovery of vulnerabilities and the ideas that your employees contributed. You have a plan in place should a data breach occur so that bad decisions are avoided during the panic of such an event. Your new *Sensitive Information Policy and Program* is in writing, and all of your employees attended mandatory training. Plus, you've taken measures to remind them of it on an ongoing basis. Because you've completed all these necessary steps to protect the data you have been trusted to keep private, your sensitive data will be more secure than ever.

And you've given your employees permission to watch each other's back without negative consequences. So don't be surprised if one day a subordinate reminds you to do something you should do. They are watching out for you, too, even if you're the new data security officer. **SF**

### RESOURCES

You can find numerous resources on data breaches, identity theft, and similar topics by searching the Internet. The ones mentioned in this article are a good place to start:

BTR-Security (www.btr-security.com)

Federal Trade Commission (www.ftc.gov)

Identity Theft Resource Center (www.idtheft.org)

*Robert Listerman, CPA, is president of BTR-Security, the data risk management division of Business Technology Resources, LLC. He is also a Certified Identity Theft Risk Management Specialist (CITRMS) and a member of IMA's Delaware Chapter. You can reach Bob at (610) 444-5295 or rlisterman@btr-security.com.*

*James Romesberg, CITRMS, is president of J.R. Consulting, specializing in operations consulting for business start-ups or existing businesses. A member of IMA's Delaware Chapter, Jim is a former member of IMA's Board of Directors. You can reach him at (302) 750-5924 or jromesberg@btr-security.com.*