

Creating a Culture of Security is Key to Stopping a Data Breach

By Robert A. Listerman, CPA, CITRMS*
President, BTR-Security

* Certified Identity Theft Risk Management Specialist



According to the Identity Theft Resource Center¹ the rate of data breach incidents has risen over 400% since 2005. Since 2005 over 245 million individuals have had personal sensitive information breached.

Forty four states have implemented specific laws requiring enterprises that loose data report the incident to them and provide a mitigating response. Perhaps you have even received one of those “Oops” letters, “your information was compromised...” Under the Fair Credit Reporting Act amendment known as the Fair and Accurate Credit Transaction Act (FACTA) the federal government requires securing sensitive data as part of compliance. All these legislative acts impose penalties and open doors for civil liability for mishandling sensitive data. Size of enterprise is not an excuse, so even a self-employed individual is not exempt.

According to CIO magazine, a technology industry trade journal, *“if you experiences 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 hiring lawyers!”*²

When an enterprise implements a program to secure sensitive data the traditional focus is on technology. They will adopt such data security improvements as having computer systems users utilize “strong passwords” or even electronic keys that create unique passwords each time they login. They will also use data encryption, and centralize critically sensitive data on a protected server. Some will even segregate internal servers from Internet access.

All that is good, however the most important, yet too often overlooked, program to secure sensitive data is the human resource solution. You may ask: human resource solution? Absolutely, the need to increase the enterprise’s “Culture of Security” will override any of the most expensive electronic or even physical security solutions.

Here’s an analogy. I attended a church retreat weekend a few years ago. As we moved from the main program area into small group rooms we left recent purchases, and some women even their purses, behind. People finished their small group assignments at different times so people wandered in and around freely until the main program re-started. Not one incident of lost or stolen items. Would you do the same at an Eagles’ game? Of course not, because the cultures between 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 completely mitigated by the “Culture of Security.”

Bottom line (my CPA side speaking), no matter how much you invest in high tech and physical security, if your culture of security is not given equal attention, a crafty mind or collusive conspiracy can derail your efforts to protect sensitive information. How do you create a “Culture of Security”?

It must start at the top. Even the federal FACTA compliance guidelines agree with this. Your data protection program must be started with the Board of Directors, or if no board, the CEO or owner. The Federal Trade Commission (FTC) is given the oversight of enforcement of FACTA for non-financial institutions. (Financial institution enforcement is covered by their specific regulatory authority.) In a brochure produced by the FTC, “*Protecting Personal Information: A Guide for Business*, within the “Lock-It” section, they specifically reference Employee Training.

“Your data security plan may look great on paper, but it’s only as strong as the employees who implement it. Take time to explain the rules to your staff, and train them to spot security vulnerabilities. Periodic training emphasizes the importance you place on meaningful data security practices. **A well-trained workforce is the best defense**³ against identity theft and data breaches.”

The FTC guidance continues with:

- Check references or do background checks before hiring employees who will have access to sensitive data.
- Ask every new employee to sign an agreement to follow your company’s confidentiality and security standards for handling sensitive data. Make sure they understand that abiding by your company’s data security plan is an essential part of their duties. Regularly remind employees of your company’s policy—and any legal requirements—to keep customer information secure and confidential.
- Know which employees have access to consumers’ sensitive personally identifying information. Pay particular attention to data like Social Security numbers and account numbers. Limit access to personal information to employees with a “need to know.”
- Have a procedure in place for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information. Terminate their passwords, and collect keys and identification cards as part of the check-out routine.
- Create “**culture of security**”³ by implementing a regular schedule of employee training. Update employees as you find out about new risks and vulnerabilities. Make sure training includes employees at satellite offices, temporary help, and seasonal workers. If employees don’t attend, consider blocking their access to the network.
- Train employees to recognize security threats. Tell them how to report suspicious activity and publicly reward employees who alert you to vulnerabilities.

When an enterprise implements, from the very top of the organization, these human resource guidance items, the seriousness of data security becomes everybody’s job. A key element to increasing the culture of security is to have the employees participate in the implementation and annual maintenance of the enterprise-wide data security program. They will unite under the common cause of keeping the sensitive information entrusted to you by your customers private and well guarded.

If you would like to know more about how to create a culture of security, please feel free to give me a call at 610-444-5295. We offer an initial 2 hour consultation at no charge or other obligation. You will learn how an organized approach to securing data will save you time, money, and your good reputation.

¹ Identity Theft Resource Center, <http://www.idtheftcenter.org/index.html>, under data breaches reports that reported breaches increased 47% over 2008 compared to 2007 and 415% since 2005.

² CIO Magazine, *The Coming Pandemic*, Michael Freidenberg, May 15th, 2006

³ Emphasis added.