PDSA.com

*Solutions for the Real World*

# PDSA Special Report

# Privacy for Application Developers

# Special Report Privacy for Application Developers

## Privacy Is So Important

Do you store information about your customers, clients, suppliers, vendors, and your employees on a computer system? If so, you need to be aware of different movements that are happening, at least in the United States, about keeping that data secure. Many states are enacting legislation that is going to require businesses to not only safeguard that information, but also force those businesses to notify those people if such information becomes compromised.

In many states there are now laws forcing companies to provide immediate notification to customers when **confidential information** about them has been compromised due to a breach on any computer system that stores such information.

## What is Confidential?

What's considered to be confidential personal information, you may ask? Here are some examples: Social Security numbers, Driver's License numbers or Identification Card numbers, Account numbers, Credit or Debit card numbers, etc. There are many laws in effect here in the United States such as Sarbanes-Oxley, HIPPA and many others that require data stored in computer systems to be secured. For example, some of these laws require first names, last names, and other seemingly harmless information to be stored securely.

## To Comply or Not Comply…

Now, it is your choice as to whether you choose to comply. If no one finds out, nothing happens. However, this is a civil law. So if the public embarrassment and public relations nightmare aren't reason enough to comply, there are also the lawsuits that will come from the individual(s) whose information was accessed. So you will have the risk of a class action lawsuit and unwanted media coverage.

## Steps You Should Take as an Application Developer

IT Managers and developers need to start performing an inventory of their database systems and identify where personal information is located. They then need to make a list of the applications that access this personal information. Each database and application needs to start implementing a more secure method of storing this data. If you have been developing using good N-Tier techniques over the years, you will find making these changes fairly painless as you can just modify your data access layer to encrypt and decrypt the appropriate fields in this one tier and all applications can now take advantage of this change. If you have not, then you are most likely in for a lot of work.

## An Example: Microsoft Access Databases

If you are using a Microsoft Access application to store personal data, you may be at serious risk, as this database does very little to secure data. Even if you have secured the database using the built-in tools in Microsoft Access, there are many tools that you can get on the Internet that will crack the Microsoft Access security very easily. Now may be the time to think about moving this data to a more robust database such as SQL Server or Oracle. At the very least you should consider implementing encryption in Access to better secure this data.

## Steps Your Company Should Take

You should begin planning of how to bring your database systems into line. Here are some examples of steps you might take.

1. Ensure your executive management team is aware of SB 1386 and other legislation that affects your business.
2. Ensure the appropriate and responsible employees in your company understand privacy and are either compliant or are implementing compliance.
3. Ensure your company has documented and disseminated to all employees information about privacy and how your organization is compliant and what steps must be taken in the event of a breach. Any unauthorized access of a computer and its data, constitutes a breach of a computer system.
4. Businesses have a responsibility to exercise a certain level of care in protecting its information - especially information deemed confidential. By not monitoring your systems, and thus, not detecting a breach, you can be accused of negligence.

5. In order to be prepared for such an event, you must have a policy and a plan for ensuring compliance within your company. Develop policies and procedures that tell you what to do before, during and after a breach of data security.

## Summary

Privacy policies and how you store data about your customers should be taken very seriously. Serious consequences could result by failure to secure your computer systems. Be sure your company is not at risk in this area. Perform an internal audit of all your systems as soon as you can to determine your exposure. Develop a set of policies and procedures and train all employees on what these policies are and what they need to do in their jobs to ensure compliance.

# Contact Information

If you would like to know more about the information in this special report, please contact either Paul D. Sheriff or Michael Krasowski at PDSA.

Paul Sheriff

(615) 675-4632

PSheriff@pdsa.com

Michael Krasowski

(714) 734-9792 x223

Michaelk@pdsa.com

## Company Information

PDSA, Inc.
17852 17th Street
Suite 205
Tustin, CA 92780

**Tel** (714) 734-9792
**Fax** (714) 734-9793
www.pdsa.com

PDSA.com
Solutions for the Real World