Are You Ready to Go AGILE ?
Let Hexaware help you
Hexaware TECHNOLOGIES
Learn More

Twelve questions to prevent a testing data breach

Howard Wiener, director of Professional Services at Direct Computer Resources says that answering the 12 questions he poses in this feature can help your organisation examine the challenges its faces when handling sensitive data during software testing.

Comedian Groucho Marx may be best recognised for saying that he would "refuse to join any club that would have (him) as a member." When it comes to the Data Privacy Breach Club, we embrace his witticism readily. Companies that have experienced business ramifications of the unintended exposure of Personally Identifiable Information (PII) include those in credit card processing, clothing and home goods, marketing, and gaming entertainment systems.

At this point in software development history, everyone in the testing community should already understand that using production data for testing is not only wrong, but also violates long-established rules and regulations from both governments and industry.

Still, the numbers are staggering. The San Diego, California-based Privacy Rights Clearinghouse reports that more than 542 billion records have been breached in the U.S. since 2005. And if you're thinking that you just need a better firewall or intrusion detection system, it's time to reconsider. Of those 542 billion breached records, greater than 32 million were a result of internal mismanagement, business operation failures or insider data theft. What could be more sadly ironic than concerned citizens in Tampa, Florida who purchased home security systems only to discover later that their personal information was stolen and used to file fake tax returns in their names?

The money involved is also astounding. In March 2011, the Ponemon Institute's annual study of the cost of a data breach put the price tag at $214 per compromised record. In another case, Ponemon estimated that the total exposure of an entertainment and gaming company resulting from a large data breach could total more than $2Billion.

Despite Americans' trust in legislative healthcare-related security requirements like HIPAA, another Ponemon report pegs the expense of data breaches in the healthcare system at $6 billion annually. In July, a California-based hospital system paid $865,000 to federal regulators to settle claims of unauthorised access to medical records. The complaints cover 2005 to 2009, a time during which hospital employees were repeatedly caught and fired for peeping at the medical records of dozens of celebrities.

These reported healthcare data breaches from 2005 through 2009 – a four-year time period – point the way towards other disturbing statistics. An April 2010 Accenture survey revealed that repeated security breaches are an ongoing challenge for many organisations. Fifty-eight percent of executives polled said they had lost sensitive personal information, and for nearly 60 percent of those who had a breach, it was not an isolated event during the 12-month period. In sum, companies compromised once are not bridging the security gap quickly enough to prevent additional incidents.

The cost of security

Outright expenditures resulting from data breaches encompass numerous areas, including development and implementation of new internal polices, technical remediation of data systems, increased auditing services, public relations programmes, customer notifications, identity theft monitoring services and legal judgments.

Other costs, such as lost customers, are less tangible. Even companies that pride themselves on outstanding face-to-face customer service suddenly fall short when personal data is exposed. Customers truly fear identity theft and they feel violated when they hear media reports or receive a data breach notification.

The 12 question challenge

Answering the questions below can help your organisation examine the challenges you face when handling sensitive data during software testing:

1) How does information flow across your enterprise?

2) How much customer data do you actually need to collect and process?

3) How long do you hold on to PII?

4) Do you have internal security policies related to who has access to which data?

5) Have you trained company associates about these policies and do you monitor their adherence to them?

6) Are your data privacy policies supported by relevant technology to both prevent and monitor for data leaks?

7) Are your customers aware of your data privacy policies and practices?

8) Are you using production data for testing or other non-production purposes? If so, is it being masked or obfuscated first?

9) Do you know how many copies of production data exist internally and externally with subcontractors and vendors?

10) Do your subcontractors and other vendors understand and abide by your data privacy requirements?

11) Could you pass internal and external audits?

12) How many of your company's divisions, departments and executives are involved in keeping sensitive data secure?

If your organisation is conscientious about data privacy, the questions above will not have rocked your world. If a few were difficult, it's time to do more than create a committee to study the issue.

Technology considerations

Data obfuscation is a set of processes by which production data is extracted and transformed so that it may be used for non-production purposes, such as systems development or testing, without compromising any personally-identifiable information it may contain. The trick to doing it well is to minimise the amount of work necessary, while producing a data set with the same logical relationships and characteristics as the original data. One complicating factor is that processes defined for a particular set of data structures will have to be revised if the structures are changed, which is a likely result of the systems development processes that are a primary driver of the need to obfuscate in the first place.

As you envision a new privacy initiative or work to enhance your current practices, consider this list of technology-related questions that relate to the data obfuscation process:

• Is it easy to deploy and customise, requiring minimal custom programming?

• Is it automated and repeatable?

• Can it create realistic-looking data in sufficient quantities?

• Does it maintain logical relationships identical to the original source data?

• Will it work to select and to subset data from all the types of data stores you're using, including relational, hierarchical or object databases or flat files?

• Will implementing it force you to restructure existing application data stores?

• Will it work with all releases of your operating platform(s)?

• From a cost effectiveness perspective, will it facilitate the security you're seeking while minimising business disruptions?

After reviewing the questions pertaining to privacy breaches and data obfuscation above, we have one final piece of wisdom from Groucho Marx regarding the gravity of your prospective membership in the Data Privacy Breach Club. In his 1933 film Duck Soup, Marx opined, "I've got a good mind to join a club and beat you over the head with it."

Howard M. Wiener

Director of Professional Services

Direct Computer Resources

http://www.datavantage.com/