



HURWITZ
& ASSOCIATES

Customer Benefit Report

*Compuware Solutions and
Services Facilitate Data Privacy
Compliance in the Application
Testing Environment*

By Rikki Kirzner

Compuware Solutions and Services Facilitate Data Privacy Compliance in the Application Testing Environment

White Paper Overview

Organizations are embroiled in a feverish effort to implement systems, tools, and solutions that will help them protect sensitive, private information and data based on best business practices. The sense of urgency has escalated because of the need to comply with recent security legislation. The situation is complicated because organizations need to protect data across the life cycle – from the test environment through production. However, this is proving to be harder than many organizations had envisioned. Furthermore, determining which technique should be used to disguise the data takes experience and expert knowledge that many companies just don't have. This white paper describes the magnitude of the problem and summarizes the Compuware solutions that effectively help companies address data privacy requirements in the test environment. The paper specifies a 12-step best practices approach to implementing a cost-effective and timely data privacy solution. It also details a four-phase implementation strategy that when combined with Compuware's products, will assist companies in streamlining the process of creating and maintaining test data environments to reduce risk and comply with data privacy legislation. Finally, the paper details a brief case study illustrating how Compuware's combination of tools, technology, best practices, and customized services can save organizations time and money, and help simplify the process of securing their test data while meeting legislative compliance.

Data Must Be Protected in Production and Test Environments

You have seen the headlines emblazoned in newspapers and trade magazines: identity theft; security breaches; phishing; viruses; worms; malware; unauthorized data access; spoofing; scamming. You may already be familiar with the growing list of government mandated security regulations including the Sarbanes-Oxley Act, Health Insurance Portability and Accountability Act (HIPAA), United States Gramm-Leach-Bliley Act, European Union Personal Data Protection Directive and the Australia Privacy Amendment Act. These attacks, threats, and legislation have forever changed the way corporations implement and enforce network policies, fortify hardware and software environments, and conduct electronic commerce. See Appendix A.

The amount of personal and sensitive information that can be found

"Protecting data in the test environment as well the production environment is proving to be harder than many organizations had envisioned."

"Compuware's combination of tools, technology, best practices, and customized services can save organizations time, money, and help simplify the process of securing their test data while meeting legislative compliance."

and accessed by computers is staggering. Electronic fraud is no longer just an annoyance. Often perpetuated by multiple, organized underworld groups, computer-based identity theft has now become a global concern. What is even more alarming is that the rate at which personal information is being electronically captured and stored online is outstripping our ability to protect this type of information in the face of rapid network growth and increasingly more sophisticated threats to networked computers.

Why Privacy Protection is Crucial

As online transactions reach record levels, companies in all major industries are struggling to find the most powerful tools and authentication solutions to help them prevent unauthorized access, protect critical and sensitive data, and build customer confidence in their ability to prevent theft of valuable information. Meanwhile, protecting the personal information of customers, business partners, suppliers, and employees is being legislated by government directives from around the world. While it is a business responsibility to keep sensitive data out of the wrong hands, providing high levels of protection and privacy has also become a competitive advantage and a way to build trusted customer and business partner relationships. Consequently, privacy protection is now a crucial factor in the software purchase decision.

After carefully assessing your company's investment in data privacy and security tools and equipment, do you believe your company has done enough to protect the privacy of its data? Perhaps your company also authenticates users, encrypts critical data, and hides specific data fields from certain applications. Do you really believe all your sensitive data assets are now fully protected? They may not be. Until recently, too many companies have not protected all the sensitive data that needs to be secure in every location where the data is used. The data privacy precautions that are implemented in the network and production environment must also be applied to test data and stored data. Until you have done that, no matter how much effort you have put forth to protect production data, you haven't done enough.

Protecting Data Privacy in the Test Environments

Improved security policies along with perimeter-oriented security technologies such as firewalls and intrusion detection systems and software have helped protect most types of data from unauthorized access or nonessential exposure. However, application quality assurance and testing is currently one of the areas most vulnerable to data theft, fraud, or unauthorized copying and replication. This is because testers, developers, and quality assurance employees as well as partners, offshore development and support personnel, and consultants who are participating in the testing or QA process often

"The rate at which personal information is being electronically captured and stored online is outstripping our ability to protect this type of information in the face of rapid network growth and increasingly more sophisticated threats to networked computers."

"Application quality assurance and testing is currently one of the areas most vulnerable to data theft, fraud, or unauthorized copying and replication."

use actual data to test software applications. On a daily basis, IT personnel move or duplicate copies of production data to the test environment--outside of the protection of the perimeter security technologies. The now unprotected data will be used to ensure that the application, as well as any modifications, new routines, or bug fixes made to the application, are working correctly prior to deployment. Too many organizations believe that since the data is only being used internally, it isn't necessary to adhere to the same privacy policies and procedures that govern its use in production.

In fact, data used in test environments is more accessible to IT personnel and is more likely to be mishandled or subject to inadvertent or deliberate security violations and theft. Therefore, it is necessary to "de-identify" the data that is actually used during the testing and QA phases through one or more techniques such as scrambling, aging, concealing sensitive values, replacement of the original data with meaningful readable data via translation tables, generating fictitious data, or a variety of other methods.

Data privacy must be inherent to the testing and QA process and while the data is at rest (stored on disk, in memory, or on tape). For this reason, most privacy legislation requires that organizations protect data regardless of where it is stored or actively being accessed and used. However, the task of implementing a data privacy assurance solution for data at rest can be quite challenging particularly for companies who have never previously tried to do this. They assume that buying the right technology, such as data management and productivity tools, will solve their data security problems. Unfortunately, they often learn that acquiring good tools and technology is not enough because these products only address part of the required solution. Many companies also need expert knowledge and experience to help them traverse the process of effectively managing the data as well as ensuring that it conforms to the policies and legislation governing the application testing environment and data privacy requirements.

Data Theft Can Damage Corporations

When data is misappropriated, companies have to endure the resulting negative impact on their reputations in addition to a loss in shareholder confidence. More importantly, the company is liable for the damage incurred as well as for financial reparations. For all these reasons, governments around the world have stepped in to protect the privacy of their citizens' data. It is no wonder that improving information privacy is one of the key IT initiatives for most companies and many major governments.

"Data used in test environments are more accessible to IT personnel and are more likely to be mishandled or subject to inadvertent or deliberate security violations and theft."

"The task of implementing a data privacy assurance solution for data at rest can be quite challenging particularly for companies who have never previously tried to do this."

"When data is misappropriated, companies have to endure the resulting negative impact on their reputations in addition to a loss in shareholder confidence. More importantly, the company is liable for the damage incurred as well as for financial reparations."

Best Practices for Implementing a Successful Data Privacy Solution

To be considered successful, data privacy solutions for a test environment must adhere to a well-defined, mutually agreeable plan that delineates the project's activities, tasks, timeframe, resources, and deliverables and incorporates the four-phase implementation methodology described later on in this paper. Hurwitz & Associates recommends a 12-step process in implementing the best practices that IT managers should consider to successfully facilitate data privacy compliance in a testing environment.

1. Understand the corporate data privacy requirements for your company and your industry and create a concise strategy for an enterprise-wide data privacy initiative that will protect the data that will be undergoing testing and QA.
2. Establish a task force across business units and IT to acquire knowledge about the application environment and various databases in order to ensure that the planned security implementations and the data transformations and disguises are designed to meet business requirements as well as all appropriate legislative mandates.
3. Create a step-by-step roadmap backed by a proven security methodology that will serve as the blueprint for implementing and supporting enterprise data privacy objectives. Make certain that the solution can be applied and enforced across a wide variety of business domains, as well as by developers, partners, offshore development and support personnel, and consultants. The solution must be applicable to all types of data used within your organization.
4. Perform a thorough baseline assessment of the data and applications to determine the scope and magnitude of the project, the required manpower, and the available resources.
5. Create a timeline detailing when your organization intends to install and deliver data privacy solutions. Provide adequate planning for the time and resources for each phase of the project.
6. Clearly identify the deliverables required to structure the transformation of the data according to the project's parameters. Be certain that even when the data has been transformed or disguised, the application can recognize its appropriate format for the specific routines that need to process the data to ensure the testing will be successful.

"To be considered successful, data privacy solutions for a test environment must adhere to a well-defined, mutually agreeable plan that delineates the project's activities, tasks, timeframe, resources, and deliverables and incorporates the four-phase implementation methodology described earlier."

7. Select proven tools that can produce and deliver data with the integrity, quality, consistency, and ability to conform to the parameters of your applications and that will meet your data privacy criteria. Organize the resources, and manage the progress of the project's activities.
8. Analyze and understand the sensitive information for each application, as well as the data structures, the appropriate data and application relationships, the selection criteria for extracting production data samples, the best disguise method, and the target test environment to be loaded.
9. Design the strategies that will be used to disguise test data and define the relevant parameters, including the data relationships between required files/tables, the selection criteria for data extraction processes, the naming convention for all supporting files, and the applicable security rules.
10. Develop and build the processes that will disguise the test data as well as the techniques that will be used to scramble information, conceal sensitive values, replace data, age data, provide fictitious data, etc.
11. Test, deploy, and maintain the data protection processes. Provide a central repository for storing and documenting all the information collected throughout each phase of the process.
12. Don't be afraid to find and hire experts with the knowledge and experience to guide you through the process of effectively managing the data and making certain it conforms to the existing policies and legislation. As many organizations face these challenges for the first time it is often difficult to know how to initiate a project of this magnitude. Getting started generally takes longer than expected. This is why the usage of data management and productivity tools is only half of the solution for implementing data privacy assurance in the test environment. Experienced professionals will save time and money by avoiding common pitfalls and problems if you aren't certain about how to proceed.

Compuware's File-AID Product Family for File and Data Management (FDM)

Compuware provides a family of integrated software products, established processes, along with consultants and services professionals who employ best practices, to enable IT organizations to create and implement a comprehensive data privacy solution. For companies that understand their data disguise requirements and the process to bring their data into compliance, Compuware has the tools

"Don't be afraid to find and hire expert knowledge and experience to guide you through the process of effectively managing the data and making certain it conforms to the existing policies and legislation."

"Compuware provides a family of integrated software products, established processes, along with consultants and services professionals, who employ best practices that enable IT organizations to create and implement a comprehensive data privacy solution."

that can help them secure the privacy of their data. If companies need more than just the tools, they can also work with Compuware's experts and best practice methods to help them implement their data privacy solutions more quickly.

Compuware's File-AID data privacy products are comprised of an integrated solution that allows companies to acquire, disguise, or load data for one or more development, test, and QA environments. When these products are combined with Compuware's solutions for application development and quality assurance including Xpediter/Dev Enterprise, Xpediter/Code Coverage, Program Analyzer and QACenter, they deliver the practical balance of processes, and tools for finding and securing sensitive data in the testing process.

Achieving Data Privacy Using Compuware's File-AID Products

File-AID/CS, File-AID/RDX and File-AID/Data Solutions are the heart of the File-AID product line enabling users to work effectively with data and secure its privacy. Together these products provide an enterprise-wide data management workbench for defining and applying disguise rules to test data. Along with other capabilities, these products offer the following capabilities:

- File-AID/CS simplifies the complex task of managing test data in multiple distributed environments, using a single, common interface. It facilitates the acquisition of the right set of source data, to intelligently disguise, populate, and refresh target test environments of the same kind, or across different structures and platforms.
- File-AID/RDX is the related data expert tool for extracting and loading a relationally intact subset of DB2 tables and MVS files for preparation of mainframe test environments. Its relational capabilities and its seamless and secure integration with the data disguise features of File-AID/Data Solutions facilitate the creation of quality, fictionalized data, while maintaining integrity, consistency, and usability.
- File-AID/Data Solutions provides the data disguise functionality on the mainframe and serves all data privacy requests originating from its own criteria rules, from File-AID/RDX, or from third-party applications, using encryption, translation, masking, aging and generation techniques.

The entire Compuware File-AID product suite enables organizations to simplify the tasks of implementing data privacy. The suite manages the processes involved throughout the data privacy life cycle entailing

"File-AID/CS, File-AID/RDX and File-AID/Data Solutions are the heart of the File-AID product line enabling users to work effectively with data and secure its privacy."

the analysis of the current application, the design of the privacy strategies, and the development and delivery of data privacy solutions. The following four examples demonstrate how other capabilities and products in the File-AID suite can simplify the implementation.

- File-AID/Data Solutions aids in the analysis and validation of data content to assist in determining value domain preservation requirements. It also integrates with File-AID for IMS to disguise hierarchical IMS databases.
- DBA-XPRT for DB2 provides impact analysis reports that cross-reference all DB2 programs and associated data objects to determine the scope of the disguise efforts. It can also manage and create target test DB2 environments.
- File-AID for DB2 assists with the analysis of SQL helping users to better understand DB2 object associations and processing rules. It inspects DB2 table data to determine data content.
- File-AID/MVS examines data files and structures to help users understand sensitive data forms and manage MVS datasets. File-AID/MVS also assists in the generation of validation reports for JCL and source code to identify inconsistencies between environments when processing sensitive data fields.

In the early stages of a data privacy project, code analysis plays an important role in determining the disguise strategies necessary to process sensitive data. Compuware products such as Xpediter/DevEnterprise, Xpediter/Code Coverage and Strobe are integrated to facilitate the automated discovery and analysis of data flow relationships within and between applications to determine the data needed to thoroughly test the application. This enables only the minimum required test data to be used, and thus reduces the amount of production data that could be exposed. Xpediter/Code Coverage also verifies and validates that coverage remains consistent with the pre-disguised or production environment.

Application quality assurance may also influence the data privacy decision-making process in the design phase. Compuware QACenter products manage test requirements and test plans that provide information regarding conditions that sensitive data must meet.

Compuware's Four-Phase Implementation Methodology

One of the first challenges organizations face when trying to protect test data involves identifying and understanding all the processes required to initiate and successfully complete a project of this magnitude and complexity. Consequently, many companies begin this

"Compuware products are integrated to facilitate the automated discovery and analysis of data flow relationships within and between applications to determine the data needed to thoroughly test the application."

"Many companies underestimate the scope of the tasks to be accomplished, and quickly realize that they are in over their heads. This type of project almost always takes longer than expected to complete."

process, underestimate the scope of the tasks to be accomplished, and quickly realize that they are in over their heads. This type of project almost always takes longer than expected to complete. Much time is wasted trying to figure out the techniques involved in acquiring the data, and knowing how to disguise it.

It is important to grasp the complexity of the relationships between data that must be secured and maintained. Companies often have difficulty knowing how to acquire and load the data into the tools or how to perform the type of analysis that will enable the tester to verify that the disguised or transformed data will actually be able to meet the objectives that were defined and required by the application parameters as well as by their organization's security goals, policies, and legal regulations.

Compuware is able to address these data privacy challenges faster and more cost effectively through a combination of its service professionals, family of tools, and its own four-phase implementation methodology that includes: Analysis, Design, Develop, and Deliver tasks. It integrates the management of a fictionalized data preparation project into the data privacy initiatives across the enterprise. This facilitates task planning, resource organization and management of the progress of the project's activities. Compuware's methodology is incorporated into templates written in project management software with embedded forms that allow every deliverable to be documented. When used in conjunction with Compuware's products, it provides a central repository for storing and documenting all the information collected throughout each successive phase of the process.

Phase 1 - Analysis

The first and most critical phase in implementing a data privacy solution is the Analysis phase. Due to the complexity and variety of business applications within each organization, the analysis phase of a disguise project is frequently the most time-consuming of the four phases. Most organizations deploy a variety of test data environments to test different business applications that are being developed or are undergoing maintenance. To thoroughly test and validate the application, these test data environments must exactly duplicate the production environment.

Locating and getting the correct test data is often difficult for developers and testers. The intricacy of finding and understanding the private and personal content of test data that needs to be desensitized is even greater. Understanding the data's relationship to other files and databases that must be synchronized presents an even greater challenge for most developers and testers. The type of information that must be collected, documented, and analyzed during this phase

"Compuware is able to address these data privacy challenges faster and more cost effectively through a combination of its service professionals, family of tools, and its own four-phase implementation methodology that entails Analysis, Design, Develop, and Deliver tasks."

"The most critical phase in implementing a data privacy solution is the Analysis phase."

"To thoroughly test and validate the application, test data beds must exactly duplicate the production environment."

includes:

- Applications to be treated
- Involved data structures
- Existing data relationships
- Sensitive data elements
- Processes acting upon/impacting sensitive data
- The scope of the target environment

Documentation should include the identification of specific individuals or groups that need the data, the frequency for refreshing test data, the conditions the test data must meet, and the specific business rules that apply to sensitive data elements. The documentation should also detail existing testing requirements as well as the processes used to extract, disguise, and load each set of test data in the test environments.

Phase 2 - Design

As in the Analysis phase, the Design phase requires more effort than selecting a few fields to scramble in a file. It contains the definition and specification of procedures that will be used to obtain the source data, desensitize, disguise, or generate replacement data, as well as the specific details for populating the target test environment with the cleansed data. The steps involved in the Design phase include defining and documenting the following:

- Application disguise strategy and process
- Field-level obfuscation rules (scramble, translate, age, generate)
- Source extract criteria for data (filters, naming conventions, etc.)
- Security rules for supporting files
- Structure, value domain (content), population strategy for translate tables
- Target environments and load methods to be used

Phase 3 - Develop

The Develop phase is where design becomes a reality. It employs the technology and right tools in an iterative progression to build, test, validate, and refine data privacy compliance processes to quickly produce results while meeting the needs of each specific data disguise rule. There are three steps involved in this phase.

The first step in development is the acquisition of the source data. This involves understanding the existing complex relationships in order to construct the correct extraction processes, and subsequently

"The Design phase includes the definition and specification of procedures that will be used to obtain the source data, desensitize, disguise, or generate replacement data, and the specific details for populating the target test environment with the cleansed data."

"The Develop phase is where the design becomes a reality."

"The Deliver phase provides a process that is well documented, repeatable, and can be audited for compliance."

apply subset and selection criteria techniques to obtain the right dataset.

The second step is building the actual disguise rules down to the field level, according to the strategies defined as a result of the analysis and design work.

The third step is getting the disguised data to its final destination while utilizing a useful load process that produces quality test data that maintains integrity and offers consistent results.

Phase 4 - Deliver

The Deliver phase involves the implementation and execution of the data privacy project within the organization's test cycles. By this time, the Analysis phase has been completed, the extract, disguise, and load strategies have been designed, developed, tested, and validated; and now the process can be deployed across the different test environments.

Once this process is completed, the developer or tester will have valid, desensitized data that meets the needs of the application to be tested. More importantly, a process now exists that is well documented, repeatable, and can be audited for compliance.

Case Study: Large National Health Care Provider Turns to Compuware's Professional Services

Compuware's combination of tools, professional services, and expertise were used to successfully help one of its large customers to implement a data privacy solution in less time and with less effort than the customer could have accomplished on its own. The customer, a national health care provider, was searching for data privacy solutions that would help it meet its HIPAA objectives in advance of the HIPAA deadline. One of its objectives was to implement a solution that would assist them in securely transmitting sensitive data to different locations around the company, as well as to an offshore partner in India that would be helping it make modifications and updates to many of their applications. The company was concerned about the liability of exposing and transmitting sensitive production data that included medical record numbers, diagnoses, Social Security numbers, and home addresses of customers and employees during the testing phase and when sending data to its contractor in India. It had to disguise key data fields to comply with federal requirements and to verify it could process all the different types of transactions required by HIPAA.

The health care provider maintains a very complex, heterogeneous

"Compuware's combination of tools and professional services and expertise were used to successfully help one of its large customers to implement a data privacy solution in less time and with less effort than the customer could have accomplished on its own."

"Compuware could provide the expertise that the health care provider lacked, and was able to help it determine the optimum strategy for treating each type of data field."

environment comprised of a number of technologies and over 1500 applications that it has to support and bring into HIPAA compliance. Its environment contains a mixture of mainframes, Windows NT, and UNIX, a variety of complex software applications, and databases including Oracle, VSAM, QSAM, DB2, SQL Server, and Sybase, among others. The health care provider had considered developing its own solutions, but quickly realized it needed experienced help with this project.

The data used for testing had to be protected and disguised before work on the application and the data could be transferred to the offshore site or used in testing the new modifications and applications that were being developed. Compuware had the proprietary encryption, translation, and aging schemes it required to disguise the data used in its testing environments. Furthermore, Compuware could provide the expertise that the health care provider lacked, and was able to help it determine the optimum strategy for treating each type of data field.

Compuware performed a proof of concept (POC) engagement that included tackling specific requirements for extracting and disguising production data to be used for application testing. Compuware worked with each of the different database groups within the healthcare company to find where the data files and tables were located and identified what needed to be disguised. The POC efforts consisted of installing Compuware's product, making sure everything was set up correctly, training the health care provider employees, and working through different exercises to illustrate how to work with the tool and then documenting what had been accomplished.

One major concern involved the ability to disguise the same record exactly the same way in whatever other database that record also existed. Whatever data protection solution was applied in one record had to be applied in every instance of that data to ensure that the same data records would be treated consistently in every location throughout the enterprise.

Compuware helped the health care provider meet each one of its major challenges and worked out solutions that would be applicable across the entire enterprise for all its applications and data security requirements. Compuware has created a working set of policies, procedures, and documentation that the health care provider will be using to convert the remainder of its applications to bring them into full compliance with HIPAA mandates.

"Compuware helped the health care provider meet each one of its major challenges and worked out solutions that would be applicable across the entire enterprise for all its applications and data security requirements."

"Protecting the privacy of personal information in the test environment is more than just a product differentiator for software vendors—it is required by recent legislation. More importantly, protecting sensitive data is an essential business obligation."

Conclusion

Protecting the privacy of personal information from customers, suppliers, partners, and employees particularly in the test environment is more than just a product differentiator for software vendors—it is required by recent legislation. More importantly, protecting sensitive data is an essential business obligation. However, achieving this goal is not easy primarily because one solution or approach to securing data privacy does not fit all applications and all industries. For that reason, many companies should consider a data privacy solution from a vendor like Compuware who offers expert knowledge services, as well as good tools.

Compuware has created an enterprise data privacy solution encompassing products, people, and proven best practices. Compuware's data privacy solutions, four-phase methodology, and experience make it possible for companies to accelerate the process of creating and maintaining secure test data environments while reducing their risk, time, and costs of bringing data and applications into full compliance with recent data privacy legislation.

Appendix A: Global Data Privacy Legislation

Data privacy has become a major global concern affecting applications, databases, operating environments and platforms of companies and organizations around the world. The following is a small subset of some of the leading privacy legislations along with their URLs where you can learn more about these legislative acts and other relevant information.

Country Privacy Legislation	URL for More Information
Australia Privacy Amendment Act of 2000	www.privacy.gov.au/act/
Canada Personal Information Protection and Electronic Documents Act and Privacy Act	http://privcom.gc.ca/fs-fi/02_05_d_15_e.asp
European Union Personal Data Protection Directive 1998	www.dataprivacy.ie/6aii.htm
New Zealand Privacy Act of 1993	www.privacy.org.nz/
Hong Kong Personal Data (Privacy) Ordinance of 1995	www.pco.org.hk/
Japan Data Protection Directive	www.alo.jp/062003RY.pdf
United Kingdom Data Protection Act of 1998	www.dataprotection.gov.uk
United States Gramm-Leach-Bliley Act of 1999	www.ftc.gov/privacy/glbact
United States Health Insurance Portability and Accountability Act of 1996	www.hipaa.org
United States Sarbanes-Oxley Financial and Accounting Disclosure Information Act	http://www.sarbanes-oxley.com/

This paper was created for Compuware Corporation by Hurwitz & Associates--a research, analysis, and strategic advisory company serving the IT industry. Its author, Rikki Kirzner, is a Partner in Hurwitz & Associates with almost 30 years experience in the computer industry providing business and data analysis, strategic direction, product messaging and positioning and business advisory services. Contact

her at rikki.kirzner@hurwitz.com.