



*"The Perfect Fit for
Your Business"™*

ROBERT H. CARPENTER, JR.

ATTORNEY AT LAW
5912 CASTLEBAR LANE
PLANO, TEXAS 75093

—
TELEPHONE 972.473.4834

—
email: Bob.Carpenter@CarpenterLaw.net

—
www.CarpenterLaw.net

January – February 2008

It's 11 O'Clock; Do You Know Where Your Data Are?

An overwhelming number of organizations use live data for testing and development purposes. . . . 69 percent use live data for testing of applications and 62 percent of respondents use live data for software development. . . . a large number of organizations may be putting live data at risk . . .¹

As companies grapple with the challenge of protecting their customers' private data, the new research shows that the cost of failing to do so is on the rise. . . . \$197 per compromised customer record in 2007, compared to \$182 in 2006.²

Data privacy and security were hot topics in 2007 and, no doubt, will remain in the headlines for years to come.³ Most businesses have been keeping up. But, maybe, just maybe, organizations – those outsourcing and those developing and testing applications – have overlooked the “not so obvious.”

Pilgrim's Progress

Ouch!, the July – August 2005 newsletter, suggested a new performance measure or SLA

¹ PONEMON INST., LLC, THE INSECURITY OF TEST DATA: THE UNSEEN CRISIS, UNITED STATES SURVEY 3 (2007), available at http://www.compuware.com/dl/TestDataReport_Final5_660png.pdf [hereinafter PONEMON SURVEY].

² Press Release, PGP Corp., Vontu, Inc. & Ponemon Inst., LLC, Ponemon Study Shows Data Breach Costs Continue to Rise (Nov. 28, 2007), http://www.ponemon.org/press/PR_Ponemon_2007-COB_071126_F.pdf (last visited Jan. 20, 2008) [hereinafter Ponemon Press Release].

³ In fact, data security breaches have been headline news since 2005. See *Ouch!*, CARPENTER LAW OFFICE CLIENT NEWSLETTER (Robert H. Carpenter, Jr., Plano, Tex.), Jul. – Aug. 2005, http://www.carpenterlaw.net/images/Ouch!_Jul._-Aug._2005_2007.pdf for a recap of 2005 events and a discussion of data security and confidentiality [hereinafter *Ouch!*].

to better define the data security perimeter, but detailed SLAs for data security have not gained traction. After some states enacted data breach laws, most information technology outsourcing contracts have included a provision like this one:

Provider has implemented and shall maintain appropriate measures designed to meet the objectives of the information security standards imposed by law or issued, whether by regulation or guideline, by any federal or state regulatory agency having jurisdiction over Customer's affairs. These measures will include, but not be limited to, disposal of consumer information as required and taking commercially reasonable actions to address incidents of unauthorized access to Customer's sensitive customer information including, but not limited to, notification to Customer as soon as possible of any such incident, which notice shall include a description of the effect of such incident on Customer's sensitive customer information and the corrective action Provider has taken or plans to take in response to the incident.

The industry typical provision is a far cry from an enforceable SLA. It is, rather, a moral imperative that may fall short of the clarity required for effective enforcement or may fail to stay abreast of the newest technology.

Ownership and confidentiality provisions, like the one below, are nestled among the many provisions in information technology contracts:

Recipient agrees to hold as confidential all Information it receives from the disclosing party (the "Discloser"). All Information shall remain the property of Discloser or its suppliers and licensors. Information will be returned to Discloser at the termination or expiration of this Agreement. Recipient will use the same care and discretion to avoid disclosure of Information as it uses with its own similar information that it does not wish disclosed, but in no event less than due care. Recipient may only use Information in accordance with the purpose of this Agreement. Provider specifically agrees that it will not use any non-public personal information about Customer's customers in any manner prohibited by Title V of the Gramm-Leach-Bliley Act or the regulations issued thereunder.

Under this ownership and confidentiality provision, a service provider is severely restricted in how it may use its customer's data – "only . . . in accordance with the purpose of this Agreement." But what does that functionally mean?

Loophole

The *Ponemon Survey* focuses on applications testing and development. Software applications development and testing requires, for maximum efficiency and reliability, the complex and robust test data that only real life data can supply. Of course, the easiest place to get such data is from customers.

To protect customers' rights in their data, "best practices" far ahead of their time have been around for several years: First, obtain the express permission of each customer to use its data in applications development and testing. Invite members of the user group to participate in the program and to "contribute" their live data to the effort. Inform



participants how their data will be used and protected in the process. Second, apply a commercially available tool or proprietary algorithm to live customer data to effectively disguise or “anonymize” it.

Setting adequate perimeter controls takes on added significance when one considers this – 89% of companies that use live data for applications development and testing use customer records. And, only 15% of such companies use either dummy or “anonymized” data. Moreover, live data used in development and testing has been lost or stolen in 23% of such companies; and 38% were unsure whether any live data had been lost or stolen.⁴

Eight-one percent of Ponemon Survey respondents reported that their companies rely upon contracts to place liability for lost or stolen data files on the outsourcer.⁵ However, effective risk allocation requires a clarity that general data security and privacy clauses do not provide. In fact, the widespread use of live data in application development and testing strongly suggests that outsourcers and their contractors do not perceive such clauses as prohibiting the practice. A more effective and clear control is necessary.

Free Sample

How often do you really get anything for “free”? Here is a provision that can be added into an information technology services contract for additional protection:

Provider agrees that it, and its independent contractors, will not use any of Customer’s Information for the development or testing of any software application without the express written consent of Customer. The foregoing prohibition includes the use of Customer’s Information regardless of whether such Information is current or not and regardless of whether such Information is encrypted or disguised through the application of any tool to anonymize such Information.

Now, if this all seems to be overkill, consider the magnitude of the risk. In 2007, the average per-incident cost of a data breach was \$6.3 million.⁶ Of course, a contract is only one of many tools to protect data. Effective vendor due diligence, on a continuing basis, should target customer data use and data security measures.

Perimeter controls to ensure against data breaches must include, among others, technology solutions such as the use of encryption and physical and logical security, and management initiatives such as security event management and personnel assurance programs. Information technology services providers must employ an enterprise-wide approach.

© 2008 Robert H. Carpenter, Jr.

This client newsletter is for informational purposes only, and is not intended to be legal advice. Transmission of this newsletter is not intended to create, and its receipt does not establish, an attorney-client relationship. Legal advice of any nature should be sought from legal counsel.

IRS CIRCULAR 230 DISCLOSURE: Notice regarding federal tax matters: Internal Revenue Service Circular 230 requires us to state herein that any federal tax advice set forth in this communication (1) is not intended or written to be used, and cannot be used, for the purpose of avoiding penalties that may be imposed by federal tax laws, and (2) cannot be used in promoting, marketing, or recommending to another person any transaction or matter addressed herein.

⁴ PONEMON SURVEY 4.

⁵ PONEMON SURVEY 6.

⁶ Ponemon Press Release.