

Software Development Times

Guest View: Insurance for the cloud

By Scott Godes and Idan Ivri

January 1, 2010

Software developers entering the field of cloud computing may need to reconsider their liability insurance coverage as they shepherd increasing amounts of user data.

Cloud computing is a loose term, but it generally refers to storing user data or applications on a remote server rather than on users' own systems. A 2009 industry study by Coda Research Consultancy estimated that, by 2015, various forms of such software could represent 17% of all information technology spending worldwide.

Consumers benefit from cloud computing because it allows them to forego expensive, all-inclusive software suites and use the Web to selectively purchase the software features they actually use. Consumers can also run Web-based software on less-expensive systems because the processing largely occurs elsewhere.

But there are potential drawbacks as well. Cloud computing necessarily gives the user less control over his or her own data, meaning that the software developer or provider may be the only line of defense for the information. There are risks that developers and data/application hosts should keep in mind.

For example, if developers make privacy the top priority, cloud-computing developers may face those that say they should be liable for the bad behavior of unsavory customers seeking a dark place to host illegal data or viruses.

On the other hand, privacy standards that are too low could make developers liable for data theft against legitimate users, or for putting private data into the hands of advertisers. Developers will also have to handle disruptions or unavailability of data and services to end users.

Do developers have insurance that would cover such risks? Any combination of these situations may lead to consumer lawsuits against cloud-computing providers or developers. Developers, in turn, will likely turn to their liability insurers for support. For that reason, developers would do well to anticipate the arguments that liability insurers commonly make to deny coverage in software-related cases.

The first policy to look to in light of these risks is commercial general liability or a business owner's policy. Those policies are commonly bought by companies of all sizes. The liability portion of those policies provides coverage to the company against lawsuits or claims filed by third parties.

One of the areas covered under such policies is for property damage allegedly caused by the developer's products. Claims alleging damage to hardware are covered under such policies; claims alleging damage to software and data should be covered, but court decisions are somewhat uneven on that question.

Courts have split on the fundamental question of whether data corruption represents "physical damage to tangible property." The common-sense approach holds that, because computers invariably record data by some electrical or mechanical action on a medium, any corruption must be "physical." But some courts have taken the opposite position.

For risks relating to invasion of privacy and data breaches, another section of general liability or business-owner policies apply: coverage for "personal & advertising injury." Personal & advertising injury coverage applies to alleged liabilities arising out of, among other things, the violation of privacy rights.

If there is a data breach, or private, personal or business information has been disclosed, there may also have been a violation of privacy rights beyond the publication of information to people who should not have it. If so, personal & advertising injury coverage may apply.

A 2009 decision from a federal appeals court in California (Netscape Communications v. Federal Insurance Co.) is favorable to online service providers, holding that personal & advertising injury coverage applied to allegations that an online service provider intercepted and internally disseminated private online communications. That holding applies with equal force to the potential disclosure of information in cloud-computing contexts.

If data was stolen or there was malicious hacking into the cloud, then a criminal/fidelity policy may also provide coverage. Such policies may be designed to address cyber-crime or to offer computer fraud endorsements that add cyber-crime coverage to a more generalized policy.

For risks relating to interruption of service and interruption of business, developers should consider first-party all-risks coverage, which may also be found within a business owner's policy. First-party policies that provide business interruption, business income and contingent business interruption coverage provide protection against losses that could apply to cloud-computing incidents.

A business' error & omission policy may provide further protection. An error & omission policy should provide coverage for liabilities relating to "professional services," and it could prove valuable in the context of cloud-computing risks.

In sum, cloud computing may represent a new trend in information technology, and a move away from established software brands. As such, it may well be a highly lucrative

new market. But with such opportunity comes risk. Policyholders should be familiar with their coverage, become familiar with malware precedents, and be aware of how best to counter arguments that insurers commonly make.

Scott Godes is an attorney with Dickstein Shapiro LLP, and he is the co-head of the firm's Cyber Security Insurance Coverage Initiative and co-chair of the American Bar Association Computer Technology Subcommittee of the Insurance Coverage Committee of the Section of Litigation. Idan Ivri is an associate with Dickstein Shapiro.

© Software Development Times. Reprinted with permission.