

technology report

VICTOR O. SCHINNERER & COMPANY, INC.

Information and Risk Management Ideas for Technology Professionals

WORKING IN THE CLOUD

Your web app may be vulnerable—and that could be costly.

IT used to be that a cloud was something in the sky, or a troublesome problem that hung over your head. No longer. Now it's the way more and more companies do business.

Welcome to the age of cloud computing. From Google apps to note-taking programs to customer relationship management software, organizations and individuals are gradually trading out their stand-alone programs for the cost savings and global access provided by online applications. A June 22, 2009, *Wall Street Journal* article said that sales of online software, which still account for only a fraction of overall software sales, are rising 40% per year compared with just 3.4% for the software market overall.

This move to the cloud brings with it a host of new security challenges for companies—particularly the technology firms, systems designers, programmers, and other tech specialists who design, market, and sell these products.

Indeed, security attacks are prevalent and on the rise. According to Qualys (www.qualys.com), an online security vendor, 55% of all security vulnerabilities discovered affect web apps. More troubling: 75% of the time there is no available patch to solve the problem. Typical problems include insufficient or weak password recovery validation, poor session

expiration protocols, and insufficient authorization. Another big problem: vulnerabilities that enable a hacker to hijack a web app, including inserting malicious code or links.

And the stakes are high. From trade secret and credit card theft to industrial espionage, software breaches can cost companies millions of dollars to explore, solve, and make customers whole. The average total cost of a data security breach was \$6.65 million in 2008, according to the *U.S. Cost of Data Security Breach Study* conducted by PGP Corporation and The Ponemon

“There are specific polices...to protect technology companies in the event of certain types of security breaches.”

Institute. Included in these figures are the costs of notifications to potential victims that their private information was breached, and the risk mitigation costs such as providing free credit monitoring to all potential victims. The most costly effect of a data breach is the cost of lost business of your clients who suffered the breach—\$4.59

million on average. When customers suffer costs like these, they will look to recoup those losses through their technology vendors. Defense costs alone can easily exceed \$250,000.

Manage Your Risk—With Protection and Sound Processes

Whether you developed the software, customized someone else's, or are otherwise responsible for it, you could be liable if something goes wrong.

“If you're developing the software and you put it in the marketplace, you could face liability if there are security breaches,” says John Gonzo, managing partner of the New Jersey law office of Kaufman, Dolowich, Voluck, and Gonzo. “Depending on the impact on the company whose data is breached, the financial ramifications to your business could be considerable. The best solution: don't leave a door open to start with.”

Gonzo recommends that tech firms implement sound business practices, including internal protocols with multiple layers of security. The idea is to have a lengthy checklist from one layer to the next that covers everything from accountability to quality control to a security audit. And somewhere in there you should be trying to break your system to identify any vulnerabilities before a hacker does.

Although sound design, best technology practices, and internal

WORKING IN THE CLOUD (cont. from front)

processes are essential, sometimes disaster still strikes. That's where a good insurance policy comes in. While basic business insurance will rarely cover technology breaches, there are specific policies to protect technology companies in the event of certain types of security breaches. To safeguard your business assets, consider purchasing a supplemental technology insurance plan.

A technology insurance policy covers third-party damages. In other words, it is designed to act if your client suffers a loss because your software application was hacked or otherwise compromised. A typical policy covers both unauthorized access to or use of a computer, software, network, or portable electronic device (think

iPhone). It also covers you if your software was the cause or the conduit for introducing computer viruses or malicious code into your client's system.

Lawsuits are very costly to properly investigate and defend. They are also very time consuming. Insurance can bring you peace of mind, along with tech experts to investigate the claim and legal experts to defend your company. Because the real culprits—the hackers—are difficult to track down and typically don't have deep pockets, it's important that you're covered if someone compromises your cloud-based software program. ♦

TechVantage thanks John Gonzo, managing partner of the New Jersey office of Kaufman, Dolowich, Voluck, & Gonzo for his assistance: Court Plaza South, 21 Main Street, Suite 250, Hackensack, New Jersey, 07601; tel: 201-488-6655; email: jgonzo@kdvglaw.com.

The information contained in this publication is based on sources we believe reliable, but we do not guarantee its accuracy. This information provides only a general overview of subjects covered; is not intended to be taken as advice regarding any individual situation or as legal, tax, or accounting advice; and should not be relied upon as such. Recipients of this publication should consult their own insurance, legal, and other advisors regarding specific coverage and other issues. © 2009, Victor O. Schinnerer & Company, Inc.

Information and Risk Management Ideas for Technology Professionals

technology report

Victor O. Schinnerer & Company, Inc.
Two Wisconsin Circle
Chevy Chase, MD 20815-7022

VICTOR O.
SCHINNERER
& COMPANY, INC.

