Chris Berg, *Senior Director, Corporate Security and Safety, Symantec Corp.*

Leslie K. Lambert, *vice president and Chief Information Officer, Sun Microsystems*

Kathleen Kotwica, *PhD, EVP and Chief Knowledge Strategist, Security Executive Council*

Derek Benz, *Chief Information Security Officer (CISO), Honeywell International*

Question: Should I allow Web 2.0 applications to be accessed from the company's computers? If I do, how do I avoid inherent risks?

Employees using Web 2.0 technologies, such as YouTube, Facebook or MySpace while at work is a growing risk for many corporations. Companies see a full spectrum of issues, including the predictable productivity losses, the introduction of viruses and exposure to malicious software attacks. Additionally, there's reputational risk relating to privacy concerns, and the evolving risk that's illustrated when employees' comments and opinions are posted to sites using company-owned infrastructure.

To prevent such problems, many companies start by rolling out a written policy — a clear statement about the organization's perspective and management's commitment to appropriately dealing with the risk. Some restrict access to Web 2.0 technologies and others are rethinking risk assessment methodologies and solutions to adapt.

Methods of communicating and collaborating by enterprise users are emerging faster than we can keep up with them. The easy answer is to shut them down, but that's not reality.

Employees are jumping on these technologies and using them to get their work done.

We decided to deal with new technologies within the framework of information security policies already in place.

Risk to your company depends on what tools are used and what company information is entered or transacted within those tools. Internal tools are likely more secure; external tools and the data stored on their systems may not follow existing company policies on how to handle company information.

For some companies, it makes sense to use Web 2.0. It depends on what the company does. A media or consumer goods company may use social networking applications to enhance its marketing reach. A start-up may use collaborative applications (e.g., IM internally) to speed up R&D. For a defense contractor, this may be too high a risk and there should be zero tolerance.

Typical policies of Internet use may already cover appropriate personal use or business use; however, if a guideline or policy was written more than five years ago, it may need updating. There is a big difference risk-wise between an employee surfing to an inappropriate content site and an employee accidentally divulging company intellectual property on a social networking site; the former is a nuisance, the latter can bring a company down.

Our company supports an internal instant messaging (IM) program, but also permits, in some cases, the judicious personal use of external IM applications, such as those that come bundled in Webmail (Gchat and Yahoo Messenger). Usage is strictly subject to our Acceptable Use Policy and Code of Conduct and can be monitored to identify/prevent leakage of sensitive data.

External social networking applications, such as Facebook or MySpace, are not permitted at this time. However we are reviewing these technologies based on growing demand from our Engineering and Marketing/Sales teams. If social networking becomes more useful in the future from the standpoint of marketing, for example, our IT, security and legal teams will consider it carefully.

NEXT MONTH'S QUESTION: Should my company seek business continuity certification under the Voluntary Private Sector Preparedness Certification Program?

For more information about the Security Executive Council, please visit www.securityexecutivecouncil.com/?sourceCode=std.
The information in this article is copyrighted by the SEC and reprinted with permission. All rights reserved.