

► COMMENTARY

Managers Beware

The use of instant messaging could be a security breach



By Scott K. Larson

For a moment, forget about office productivity and your concern that employees are chatting away on non-business related topics. Instead, focus on the volume and content of instant messages being exchanged between employees, clients and business partners. Then ask yourself these questions:

1. Does the information being exchanged on instant messaging contain sensitive human resources information or business plans?
2. Does your instant messaging platform transmit “in the clear” (without encryption)?
3. Are the messages being saved on employee hard drives or on a network server in your organization?

If the answer is “yes” to any of these questions, you should be concerned. Employees and hackers may be able to intercept and read instant messages not intended for them, putting your company at risk, not just as a practical matter but as a legal matter.

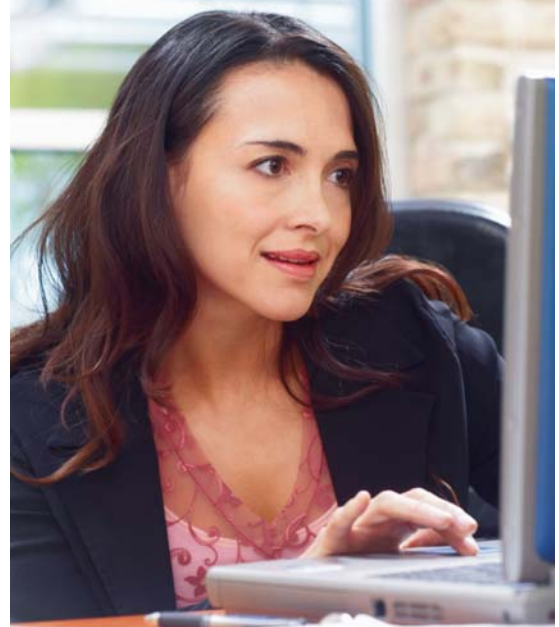
CSI Lesson

Television has taught us that forensic scientists can uncover lots of hidden evidence. In the computer world, this means that instant messages may remain on an employee’s hard drive even if the employee does not explicitly save the messages. Your computer operating system randomly saves bits of data to the hard drive, which may contain artifacts of instant messages.

More and more, lawyers are asking for e-mail and instant messages in the course of civil litigation, whether the case involves an employment dispute or a patent issue. In fact, new amendments to the Federal Rules of Civil Procedure now require production of paper documents as well as electronically stored information. Increasingly, this will include instant messages as their popularity grows and as they become part of the evolving legal and regulatory landscape of the 21st century.

What Employers Can Do

Businesses should heed the warning of one company that recently faced an instant messaging problem. Executives at the company were concerned their conversations were being surreptitiously intercepted through the telephone, e-mail or



More and more, lawyers are asking for e-mail and instant messages in the course of civil litigation, whether the case involves an employment dispute or a patent issue.

instant messaging because certain employees knew highly sensitive company information that had been privy only to senior management. A team of forensic examiners looked at three distinct stories or “vectors” of information being discussed within each communication medium and determined that the leak was coming from instant messages. The team found artifacts of the CIO’s instant messages on the hard drives of an IT staffer and his spouse. The team also located a “sniffing” device behind a desk in the IT department, a device that had been capturing all of the company’s instant messaging traffic.

To avoid these types of leaks and security issues, employers may want to consider taking the following steps:

1. If practical, eliminate or at least limit the use of instant messaging in the workplace.
2. Develop policies describing what can and cannot be discussed on instant messages, and train employees accordingly.
3. Encrypt instant messages as part of a larger information security framework.
4. Develop a plan to capture or preserve instant messages, should they be called for in litigation.
5. Perform background checks on critical IT personnel (and contractors) that have access to executive communications and other sensitive company information. **MB**

Scott K. Larson is a partner with the Minneapolis office of Stroz Friedberg, LLC, a national consulting firm specializing in electronic discovery, cyber-crime response and computer forensics.