

Privacy Officers

ADVISOR

iapp
international association of privacy professionals

The official newsletter of the International Association of Privacy Professionals

March 2004

Editor: Kirk J. Nahra

Volume 4, Number 6

IAPP Summit Report

Privacy Professionals Work to Build Professional Community

IAPP Staff Report

If you weren't one of the more than 500 privacy professionals at the IAPP Privacy & Data Security Summit last month, you missed out.

Thursday morning attendees were greeted by FTC Commissioner Orson Swindle, who discussed the commission's work with a number of critical privacy issues, including identify theft, CAN-SPAM, and the host of new domestic and international laws and regulations affecting U.S. industry. Swindle's morning keynote was entertaining, animated, and extremely informative.

Following Swindle, five international information and privacy commissioners took to the lectern to address the assembled mass of privacy professionals in the Renaissance Hotel Grand Ballroom. Canada's privacy commissioner, Jennifer Stoddart, talked about how recent events affecting the Canadian and U.S. food supplies, such as mad cow disease and Prince Edward Island pig DNA, exposed the depth of Canadian concerns related to cross-border information sharing. Richard Thomas, U.K.

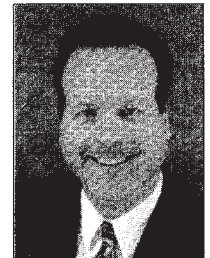
See *IAPP Summit*, page 12

Using Internet-Monitoring Technology to Secure Financial Privacy

David Fertell

The technology revolution dramatically revamped the way the financial services industry communicates with customers. Go to any bank's Web site and you will find online account access. On Wall Street you see brokers using their palmtops to instant message (IM) their clients with their latest offerings. And in some institutions, customer service

representatives use "chat" to help customers resolve problems in real time. Multiple communication channels and easy access to customer data, however, come with a high price tag.



See *Internet Monitoring*, page 6

The Information Economy's Cutting-Edge Career

David Hass, MBA, LLB, BA

Privacy laws or policies are always fundamentally based on the principles underlying "fair information practices," one of which is accountability. This principle, in its Canadian incarnation, generally states that "an organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance" with

the remaining principles, which include identifying the purposes for which information is used, maintaining its accuracy, and implementing security safeguards.

Ensuring compliance with privacy laws can be a daunting task, so

See *Career*, page 3



This month:

- | | |
|--|----|
| ■ Privacy and Data Collection Strategies | 8 |
| ■ Antispam Measures in the United Kingdom — How They Work | 15 |
| ■ ISTPA Formally Invited to Participate in ISO/IEC JTC 1 Study Group on Privacy Technology | 18 |
| ■ COPPA Overseas | 20 |

Internet Monitoring

from page 1

Identity theft was the number-one complaint received by the Federal Trade Commission in 2003, according to a published report. The FTC, which is charged with stopping business fraud and deception, said 42 percent of the more than half-million com-

plaints it logged in 2003 involved identity theft, compared with 40 percent of the 400,000 complaints in 2002. In fact, identity theft has topped the complaint list for the last four years.

This point was proven in December 2002 when a computer help-desk employee with access to sensitive passwords from banks and credit companies allegedly downloaded

personal information on 30,000 Americans, then sold that information to scam artists. Prosecutors alleged that over three years, the thieves had stolen millions of dollars using passwords to access personal information, including Social Security and bank account numbers.

Despite stories like this, many organizations fail to realize that the greatest security threat may actually

Software Points to Consider When Getting Started

There are a variety of reliable software programs available to monitor Internet use. Here are some points to consider when evaluating software:

❑ Get involved Early On

Privacy and compliance officers should be involved in the selection of data capture features to ensure that institutions comply with federal and state regulations.

❑ Make Sure the Software's Primary Focus Is Monitoring

Some software programs only filter content based on keywords. Other applications simply block communications based on a "block list" comprised of a list of "off-limit" URLs. To comply with GLBA, however, you need to be concerned about information leaks rather than communications being received, so monitoring software is more appropriate.

❑ Make Sure the Software Archives Data for Future Review

Financial institutions often need documentation to comply with federal and state regulations. Choose software that records and reports on the exact data being transmitted, rather than just an activity summary.

❑ Implement a Solution that Validates Captured Data

Captured data may be corrupted during transmission or may be altered by employees wishing to hide their actions. Select software that takes a "fingerprint" of all data as it is captured so information can be validated by individuals or entities responsible for oversight or prosecution.

❑ Choose Software that Accommodates Multiple Locations or Branches

Choose a product that is easily ported to multiple locations, without requiring additional investments in computing hardware and infrastructure.

❑ Implement an Internet Acceptable Use Policy

Clear guidelines are the first step toward ensuring employees' cooperation. Implementing an acceptable use policy communicates what is and is not acceptable for employees to do online. Sometimes simply having the policy and software in place acts as a deterrent to misuse.

❑ Look for an Automated Reporting Feature

One of the perceived disadvantages of using monitoring software is the need for staff to constantly check the software to see if misuse has occurred. Some monitoring software, however, can be set up to automatically generate reports, as often as needed.

❑ Document Everything

Because financial institutions are legally bound to keep e-mail records to protect against charges of financial misdoing and ensure proprietary information is secure, Internet-monitoring software provides an audit trail that can protect you against serious legal actions.

come from the inside. According to a survey conducted in 2003 by the Computer Security Institute and the FBI, 80 percent of respondents reported that insider abuse of the corporate network was the most cited form of cyberattack.

The Gramm-Leach-Bliley Act

To help protect consumers from identity theft and other forms of fraud, the government has responded with new laws and regulations. Leading the U.S. government's list of reforms is the Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act, or GLBA, which includes provisions to protect consumers' personal financial information held by financial institutions. Within GLBA, the financial privacy rule and the safeguards rule specifically address personal information privacy requirements.

The financial privacy rule and the safeguards rule apply to "financial institutions," including banks, securities firms, insurance companies, and companies that provide many other types of financial products and services to consumers. Among these services are lending, brokering, or servicing any type of consumer loan; transferring or safeguarding money; preparing individual tax returns; providing financial advice or credit counseling; providing residential real estate settlement services; collecting consumer debts; and an array of other activities.

The financial privacy rule governs an institution's collection and disclosure of customers' personal financial information such as names, addresses, phone numbers, bank and credit account numbers, income and credit histories, and Social Security numbers. It also applies to companies, whether or not they are financial institutions, which receive such information.

The safeguards rule requires all financial institutions to design, implement, and maintain safeguards to protect customer information. The safeguards rule applies not only to financial institutions that collect information from their own customers but also to financial institutions — such as credit reporting agen-

cies — that receive customer information from other financial institutions.

There is a great deal of incentive to comply with GLBA. Noncompliance results in a variety of fines and up to five years of imprisonment for each violation. Most firms have already established processes to broadcast privacy policies to their customers. The real area of concern, however, is the lack of appropriate technology solutions to adequately secure customer information and prevent the accidental or malicious disclosure of customer personal information.

The Internet Monitoring and Control Solution

Although information technology administrators rely on a variety of software applications and system fixes to secure financial networks, Internet-monitoring and control software is an

Despite its rising popularity as a tool for enhancing productivity in the workplace, the security issues involved with instant messaging use are scary and real.

often overlooked tool that can be used to augment existing technology initiatives.

A comprehensive Internet-monitoring software will track all widely used forms of Internet communications including Web browsing, file transfers, news group postings, chat, e-mail and IM. Internet-monitoring software allows employees to send files or e-mail, for example, and then captures data from these transmissions in order to report on the Internet activity that occurred.

Employers are provided with a detailed log of employees' Internet activities, including the content of transmitted messages. An IT administrator reviewing the log can easily spot employee use that might constitute abuse of the Internet or threaten GLBA compliance.

The most sophisticated and flexible software in this emerging class, known as global Internet management software, even allows employers to

manage the Internet use of "remote" employees, like telecommuters, traveling sales people, or those located in branch offices.

Internet-monitoring software is widely used to manage employee Internet use and ensure workers are using their employer's Internet connection as intended. The software performs double-duty by also controlling access to sensitive customer information and ensuring that this information is not leaked outside the company.

Access Management

Some Internet-monitoring products actually allow you to define user-level access to certain areas of an organization's intranet or the Internet. The IT administrator can then define rules determining which users have access to specific areas. This enables periodic audits to determine who,

internally, is trying to access customer data or who is actually attempting to send this data outside the institution. For example, an insurance agency could use Internet-monitoring and control software to

restrict access to customer account information to agents only. In this way, administrative personnel would not be allowed to see sensitive customer data.

When considering the many ways that employees can transmit information, many companies tend to focus on e-mail as the weakest link. As workers become increasingly 'Net-savvy, however, many other forms of communications, such as IM, are being introduced to the workplace.

IM has become an indispensable tool for the financial services industry, helping people make quicker real-time investment decisions. In October 2003, a group of the largest banks — including Credit Suisse First Boston, Lehman Brothers, Merrill Lynch, Morgan Stanley, and UBS Warburg, Deutsche Bank and J.P. Morgan Chase — established a group called the Financial Services Instant Messaging Association to encourage leading

See **Internet Monitoring**, page 8

Internet Monitoring

from page 7

public IM providers to adopt industry standards for interoperability.

Despite its rising popularity as a tool for enhancing productivity in the workplace, the security issues involved with IM use are scary and real. Because this is a new medium, you may lack the appropriate safeguards to protect your company from violating federal compliance rules that require all client communications to be logged and archived.

Archiving

One of the most valuable features of Internet-monitoring software is the ability to archive data automatically. Most companies today are drowning in data, and privacy regulations have only compounded the amount that must be stored and kept indefinitely.

If, for example, a breach of confidential customer data occurred at a brokerage firm, the result could be a costly lawsuit. In this case, unstruc-

ture data such as e-mail and chat conversations between brokers and their customers could be admissible in court. It is then often up to the defendant to produce these supporting electronic documents. This recovery process can be laborious, difficult, and expensive if the Internet data is not readily available in an internal archive.

Keyword Blocking

Disclosure of personal data can occur through many channels and may include the transmission of nonpublic personal information through e-mail, chat rooms, file transfers, IM, and public newsgroup postings. Internet-monitoring software can be set to block electronic transmissions based on a predefined list of keywords. So, for example, a bank could set the software rules to check transmissions against a database containing customer bank account numbers.

If the software detects any of these account numbers being transmitted outside the company, it would quickly terminate the transaction and alert IT

staff that a violation had occurred. Because the software can specifically identify transmissions both by user and by computer, it is easy to identify the person responsible for the security breach.

Monitoring Internet usage in the workplace is a reality in today's electronic economy and a necessity for mitigating risk in certain industries. It is at the intersection of protection and privacy where a thorough understanding of both the applicable regulations and appropriate technology are required to avoid exposure. ■

About the author

David Fertell is president and CEO of Pearl Software, a Philadelphia-based software company that creates Internet-monitoring software applications for both corporate and home use. Fertell has a background in data networking, software design, and robotic imaging and operations management. He can be contacted at (800) 732-7596 or info@pearlsw.com.