

IS Auditing and Information Privacy Governance: A Natural Fit

By Chris Zoladz, CISA, CIPP, CISSP, CPA

For years information systems (IS) auditors have faced the challenge of convincing business managers of the value they provide to the organization. This was often a daunting challenge. Over time, however, an evolution in general understanding and appreciation of the significant dependence on information systems for virtually every part of the business helped to raise the business's consciousness of the obvious: the security of these information systems is vital to the business, and assurance that these systems are secure is essential.

With the US Sarbanes-Oxley Act requirements, sectoral security mandates (e.g., US Gramm-Leach-Bliley Act, US Health Insurance Portability and Accountability Act), required online privacy disclosures in some states, international data protection laws (e.g., EU Data Protection Directive), myriad US state security breach notification laws and comprehensive credit card company security requirements (the Payment Card Industry [PCI] Data Security Standard [DSS]), the discussion around "why are we even talking about IS auditing?" hopefully is a distant memory. Many business managers now understand "why" it is important and are focusing more on "how" and the financial impact of how the organization addresses these needs. However, the need to continue demonstrating value to the business is a timeless and fair expectation.

This article will focus on an emerging area for which IS auditors are a natural fit for delivering more value to an organization: information privacy governance.

Information privacy is a must for the security mandates mentioned previously as well as an integral element of a number of customer-facing, revenue-generating activities. Specifically, information privacy is an integral element of key business processes surrounding e-commerce, e-mail marketing, telemarketing and doing business in certain international markets. To demonstrate this point, a brief review of e-commerce and e-mail marketing is presented.

E-commerce

For many organizations, conducting business on the Internet is usually the lowest-cost sales channel and thus the one many organizations want to aggressively expand. Secure, privacy-sensitive e-commerce is an absolute requirement to successfully establishing consumer trust, protecting an organization's brand and driving more online business. The privacy officer works with the e-commerce business leaders and information security to ensure that there is an accurate and complete privacy statement posted on the web site, so that

customers understand what information is collected, why it is collected, how it will be used, use of cookies or pixel tags, and security measures in place to protect the customer's information. If an organization's web site and associated business practices do not live up to the privacy statement, customer loss and potentially an investigation from, in the US, the Federal Trade Commission and/or a state attorney general's office can be expected. The IS audit function can help assess and manage this risk and add value, protecting a low-cost, revenue-generating sales channel, by conducting a privacy audit of the web site. IS auditors can be a natural fit for this activity as they are experts in auditing information systems and that is precisely what is needed in this case. While this article is not focused on how to conduct a privacy audit of a web site, some of the areas that should be covered are:

- Is a current privacy statement posted?
- Are the disclosures complete and accurate?
- Is the opt-out process functioning as intended?
- Is the P3P version of the privacy statement consistent with the narrative version?

*IS auditors are a natural fit
for delivering more value to
an organization: information
privacy governance.*

E-mail Marketing

Like selling products or services via a web site, e-mail marketing is often a least-cost channel for promoting products and services. However, e-mail marketing is regulated activity in the US and in some international markets. Also, and as important, poorly executed e-mail

marketing can be one of the fastest means to alienate customers. Proper e-mail marketing management includes adherence to the e-mail marketing laws and being aware and sensitive that some consumers will view e-mail marketing messages as an annoyance and intrusion. IS auditors can be invaluable to helping the business protect their e-mail marketing channel from a privacy perspective. Just a couple of the specific areas that could be assessed are:

- Were customers informed that their e-mail address would be used for marketing purposes?
- Has the e-mail marketing list been adjusted for previous opt-outs?
- How are consumer complaints about e-mail messages handled?

Gaining Information Privacy Expertise

While IS auditors can be a natural fit for providing information privacy governance, information privacy is a distinct body of knowledge and training is necessary to be

able to competently audit this area. The information privacy profession is relatively new and is being shaped by the International Association of Privacy Professionals (IAPP) just as ISACA did for the IS auditing profession a few decades ago. The IAPP was established to define, promote and improve the privacy profession globally. The IAPP is committed to providing a forum for privacy professionals to share best practices, track trends, advance privacy management issues, standardize the designations for privacy professionals and provide education. The IAPP also sponsors the Certified Information Privacy Professional (CIPP), a certification for privacy professionals.

Conclusion

Progressive value-added IS auditing will continue to evolve over time as technology and business needs evolve. A component of the current-day IS auditing repertoire should include information privacy auditing. This is a natural extension of the skill sets and focus of the current-day IS auditor.

However, this is a new subject matter area that, like any other, requires expanded subject matter expertise. As a long-time Certified Information Systems Auditor™ (CISA®), the author encourages readers to consider expanding their current activities to include information privacy governance and add more value to their enterprise today.

Chris Zoladz, CISA, CIPP, CISSP, CPA

is the vice president, information protection and privacy, at Marriott International Inc. Zoladz is responsible for information protection and privacy strategy, policy development and deployment, security awareness, and compliance strategies to meet information protection/privacy, business and legal requirements. He is a past president and current board member of IAPP and a past board member and treasurer of the National Capital Area (Washington DC, USA) Chapter of ISACA.

Information Systems Control Journal is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *Information Systems Control Journal* does not attest to the originality of authors' content.

© 2008 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org