http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 5 (1): 177-182, 2006
ISSN 1812-5638

Auditing of Information Privacy

Adel Ismail Al-Alawi and Eman Ali Hafedh
Department of Management Information Systems, College of Information Technology,
University of Bahrain, P.O. Box 32038, Kingdom of Bahrain

Abstract: Recently, it has become evident that an increasing number of organizations have been collecting data about individuals as part of their business. Moreover, advances in information technology have greatly contributed in decreasing the cost of data collection. As a result, concerns regarding privacy have become an important issue and potential obstacle to both individuals and organizations. In addition, a significant gap exists in the privacy protection for individuals. In this regard, this study enlightens the issues surrounding privacy as well as the main controls applied for protecting information privacy. Furthermore, it assesses the critical role of IS auditors with regard to the privacy protection.

Key words: Information systems, privacy issues, personal data, auditors, Bahrain

INTRODUCTION

Privacy has been defined as the right of individuals to control the collection and use of personal information about themselves[1]. The right to privacy has become one of the most important ethical issues of the information age. They have found, in their study regarding personal information privacy, that new technological capabilities plus the increasing value of information as well as the confusion surrounding the definition of what is ethically right and what is wrong are the main forces behind the growing focus on data privacy.

Organizations have been collecting vast quantities of information on individuals and as they claim this information are to build better relationship with their customers. However, a number of businesses have tended to exchange individuals' personal data with external parties without their consent. Therefore, the importance of privacy enhancing measures and controls has become evident. Thus, many Bahraini organizations have established specific procedures and practices as well as a privacy policy that enforce the protection of information privacy and consequently decrease the privacy gap and the surrounding issues.

This study aims to investigate the main issues surrounding information privacy. Moreover, it examines the main practices and controls as well as the technical and organizational measures for protecting personal data in local companies. Finally, we assess the critical role of IS auditors in relation to the protection of Information privacy.

With the increasing concerns regarding privacy, this study can provide guidance for Information Systems professionals in dealing with data privacy issues. Furthermore, the findings of this study can support IS auditors in assessing the main measures and procedures currently implemented in their companies, in order to determine whether these are effective in protecting the rights of those from and about whom they collect data. Finally, this study enlightens the critical role of IS auditors with regard to privacy protection and focuses the attention of companies and individuals on the significance of internal and external auditors in almost every organization.

Since most organizations claim that they have invested their best efforts to secure personal data, it becomes important to investigate whether these claims are right or not. Moreover, current IT capabilities to abuse personal data and the increasing concerns of individuals about threats to their personal privacy necessitate a study that answers two main questions. First, how companies make sure that personal data are treated properly and accurately. Second, what is the key role of auditing in protecting data privacy?

Based on the research framework, the following are the main hypotheses proposed as being directly related to data privacy:

H1: Individuals' concerns regarding the privacy of their personal data increase with the advent of new technologies.

Corresponding Author: Dr. Adel Ismail Al-Alawi, Department of Management Information Systems, College of Information Technology, University of Bahrain, P.O. Box 32038, Kingdom of Bahrain Tel: +973-17-437033 Fax: +973-17-770227

H2: Maintaining data privacy is one of the goals of IS auditors.

H3: Effective controls in any organization means providing better protection for personal data.

Recent media attention to information privacy issues has shown that citizens are increasingly concerned about information privacy and their right to it. Organizations have been collecting data about individuals at an increasing and alarming rate. Moreover, the ability to gather so much information on individuals is largely because of advances in Information Technology (IT).

The advent of IT increased interest in the right of privacy issue in the 1960s and 1970s. Largely due to increased surveillance potential and record keeping abilities of computer systems, laws governing the collection and handling of personal information were demanded. In 1970, the first data protection law in the world was enacted in Germany. National laws soon followed in several countries[1]. In their study regarding personal information privacy, they have found that there are three main forces driving the growing focus on personal information privacy: (1) new technological capabilities, (2) increasing value of information and (3) confusion surrounding the definition of what is ethically right and what is wrong.

Highly sophisticated technology with its enhanced capacity for communication, computation, storage, and retrieval has given personal information privacy and the right of privacy new meaning. When documents were kept in filing cabinets, control over the information was relatively easy to maintain, because physical access to files could be limited by the use of locks and guards. As computerization increased, more documents were stored on magnetic media, making the provision of security a greater problem[1].

The second driving force behind the increasing issues of data privacy is the increasing value of information. As computing and data management continue to become more decentralized and control is diffused, the value of information is increasing with new ways of using it for strategic and competitive advantage.

Organizations have found that the data collected about customers can be used to target prospects, improve customer satisfaction, and identify opportunities for new products or services. As we all know companies are increasingly targeting certain consumer segments instead of all potential buyers. In order to do this, companies need to know specific purchasing characteristics of individuals. Therefore, it is necessary to store and share information with other organizations and sometimes without user knowledge or permission.

The third driving force was the confusion surrounding what is ethically right and what is wrong. IT has changed the public's perception of privacy. Organizations are faced with completely new policy decisions. Furthermore, with the massive amounts of data being collected by business and government, privacy could easily be compromised by persons with authorized access[1].

Despite privacy laws that have been enacted in many countries, Henderson and Charles[1] note there is still a need to develop national privacy policies that address: the balance between the right to privacy and the right to access as well as the expectations of individuals and the needs of society.

In their study regarding privacy-enhancing technologies, Senicar *et al.*[2] have identified the technology that may provide satisfactory protection of privacy over general networks that are building today the information infrastructure. These technologies were known as Privacy-Enhancing Technologies (PETs). Among which is Encryption which is one of the oldest security mechanisms that can be used for provision of data confidentiality. They have also identified the digital signature, cookie management and the identity protector as being privacy-enhancing technologies.

Even with the existence of PETs, people are still responsible for protecting their personal data. Hinde[3] notes that one of the ways in which criminals obtain confidential information on individuals is through careless disposal of this information. For instance, data is left on old computers when they are disposed of. He has also suggested the best practices for consumers to help ensure their personal and confidential information remains secure.

All of the above mentioned arguments agree on one fact that is concerns about data privacy are increasing tremendously. Therefore, there is a critical need for control and audit of computers. Weber[4] identified seven major reasons for establishing an IS audit and control function in the organization. The main reasons were: (1) the organizational cost of data loss; (2) cost of incorrect decision making; (3) cost of computer abuse; (4) value of S/W, H/W and personnel; (5) high costs of computer errors; (6) maintenance of privacy and, (7) to control the evolution of computer use. Among these reasons, the maintenance of privacy was the focal point for this study. In this regard, he considered that computer professionals have a responsibility to ensure that data is used only for the purposes intended.

In relation to IS auditing, Sayana[5] noted that Information systems are the lifeblood of any large business. As in years past, computer systems do not merely record business transactions, but actually drive the key business processes of the enterprise. In such a scenario, senior management and business managers would have concerns about information systems, so the purpose of IS audit is to review and provide feedback, assurances and suggestions.

MATERIALS AND METHODS

A questionnaire was distributed to a random sample of 100 individuals with a cover letter that briefly described the study. Additionally, interviews were conducted to ensure that questionnaire responses were consistent with the underlying constructs.

Out of the 100 questionnaires distributed, 16 were blank- returned. We excluded two partially completed responses from subsequent analysis. Thus, the effective and completed responses that were analyzed numbered 82. Due to the researchers' personal contact, it took them four weeks to finish collecting surveys. An interview method was employed to collect some perceptions of IS professionals in local companies in order to acquire knowledge regarding current controls applied by these companies. The data collected for this study were analyzed using Statistical Package for Social Science (SPSS).

RESULTS AND DISCUSSION

Using the descriptive analytical tool in SPSS, it was found (Table 1) that a majority (40.2%) of the respondents were 22 years of age.

Table 2 shows that most of the respondents were females (56.1%) verses males (43.9%).

Table 3 shows that the majority of the respondents (90.2%) were bachelor holders, while (4.9%) had post graduate diploma.

The results are shown using a descriptive analytical tool which is Cross tabulations procedure. This tool forms two-way tables and provides a variety of tests and measures of association for two-way tables.

For the purpose of testing the research hypotheses, respondents were asked several questions to investigate their concerns regarding the privacy of their personal data and to see whether these concerns are increasing in the new information age. Moreover, the results of this survey were further analyzed to see whether the findings were consistent when respondents were grouped by gender, age and education.

The survey results indicate, as shown in Table 4, that individuals are very concerned about the threats to their personal privacy. A majority of respondents believed that businesses can gather personal information about consumers without their permission, including their demographic data (29.3%), types of products and services they buy (63.4%), the amount of money in their bank accounts (1.2%), and their medical history (6.1%).

Table 1: Age of respondents

Age (year)	Frequency	%	Valid %	Cumulative %
21	21.0	25.6	25.6	25.6
22	33.0	40.2	40.2	65.9
23	9.0	11.0	11.0	76.8
24	11.0	13.4	13.4	90.2
25	7.0	8.5	8.5	98.8
26	1.0	1.2	1.2	100.0
Total	82.0	100.0	100.0	

Table 2: Gender of respondents

Gender	Frequency	%	Valid %	Cumulative%
Male	36	43.9	43.9	43.9
Female	46	56.1	56.1	100.0
Total	82	100.0	100.0	

Table 3: Educational degree of respondents

		Frequency	%	Valid %	Cumulative %
Valid	Diploma	3.0	3.7	3.7	3.7
	Post Graduate Diploma	4.0	4.9	4.9	8.5
	Bachelor	74.0	90.2	90.2	98.8
	Master	1.0	1.2	1.2	100.0
	Total	82.0	100.0	100.0	

Respondents thought that current laws are inadequate to protect consumers. They were asked to agree or disagree with the following statement: Current national laws are strong enough to protect your personal privacy from businesses that collect information about consumers. Table 5 shows that 64.6% of respondents disagreed with this statement, with 17.1% agreed while 18.3% neither agreed nor disagreed.

Table 6 reveals that men (25.6%) were less likely than women (39%) to disagree that existing consumer protection laws are strong enough. While, surprisingly Table 7 shows that none of the post graduate diploma holders disagree with that.

Moreover, Table 8 shows that the majority (67.1%) believed that they have never been in a situation where a company had wrong information about them, while (26.8%) indicated that they did not know. Among (6.1%) who believed wrong data is maintained about them, Table 9 shows clearly that (80%) could correct the data while (20%) couldn’t.

Most of the respondents (64.6%) reported that they would mind if a company they did business with sold information about them to another company. Table 10 proves that women (40.2%) were more likely than men (24.4%) to feel that companies should not sell personal information about customers.

Table 4: Age of respondent * q1 Cross tabulation

		q1				
Age of respondent	Count	Amount of money	Medical history	Types of products and services you buy	Demographic information	Total
21	Total	0.0	0.0	11.0	10.0	21.0
	Percentage	0.0	0.0	13.4	12.2	25.6
22	Total	0.0	0.0	22.0	11.0	33.0
	Percentage	0.0	0.0	26.8	13.4	40.2
23	Total	0.0	0.0	7.0	2.0	9.0
	Percentage	0.0	0.0	8.5	2.4	11.0
24	Total	1.0	5.0	4.0	1.0	11.0
	Percentage	1.2	6.1	4.9	1.2	13.4
25	Total	0.0	0.0	8.0	0.0	8.0
	Percentage	0.0	0.0	9.8	0.0	9.8
Grand total	Total	1.0	5.0	52.0	24.0	82.0
	Percentage	1.2%	6.1%	63.4%	29.3%	100.0%

Table 5: Age of respondent * q2 Cross tabulation

		q2			
Age of respondent	Count	Agree	Neither	Disagree	Total
21	Total	1.0	9.0	11.0	21.0
	Percentage	1.2	11.0	13.4	25.6
22	Total	12.0	4.0	17.0	33.0
	Percentage	14.6	4.9	20.7	40.2
23	Total	0.0	2.0	7.0	9.0
	Percentage	0.0	2.4	8.5	11.0
24	Total	1.0	0.0	10.0	11.0
	Percentage	1.2	0.0	12.2	13.4
25	Total	0.0	0.0	8.0	8.0
	Percentage	0.0	0.0	9.8	9.8
Grand total	Total	14.0	15.0	53.0	82.0
	Percentage	17.1%	18.3%	64.6%	100.0%

Table 6: Gender of respondent * q2 Cross tabulation

		q2			
Respondent gender	Count	Agree	Neither	Disagree	Total
Male	Total	6.0	9.0	21.0	36.0
	Total (%)	7.3	11.0	25.6	43.9
Female	Total	8.0	6.0	32.0	46.0
	Total (%)	9.8	7.3	39.0	56.1
Total	Total	14.0	15.0	53.0	82.0
	Total (%)	17.1	18.3	64.6	100.0

Table 7: Educational Degree * q2 Cross tabulation

		q2			
Educational level	Count	Agree	Neither	Disagree	Total
Post Graduate	Total	0.0	7.0	0.0	7.0
Diploma	Total (%)	0.0	8.5	0.0	8.5
Bachelor	Total	14.0	8.0	53.0	75.0
	Total (%)	17.1	9.8	64.6	91.5
Total	Total	14.0	15.0	53.0	82.0
	Total (%)	17.1	18.3	64.6	100.0

Table 8: Age of respondent * q3 Cross tabulation

		q3			
Age of respondent	Count	Yes	No	Don't know	Total
21	Total	0.0	16.0	5.0	21.0
	Total (%)	0.0	19.5	6.1	25.6
22	Total	4.0	23.0	6.0	33.0
	Total (%)	4.9	28.0	7.3	40.2
23	Total	0.0	6.0	3.0	9.0
	Total (%)	0.0	7.3	3.7	11.0
24	Total	1.0	10.0	0.0	11.0
	Total (%)	1.2	12.2	0.0	13.4
25	Total	0.0	0.0	8.0	8.0
	Total (%)	0.0	0.0	9.8	9.8
Total	Total	5.0	55.0	22.0	82.0
	Total (%)	6.1	67.1	26.8	100.0

Table 9: Age of respondent * q4 Cross tabulation

		q4		
Age of respondent	Count	Yes	No	Total
22	Total	4.0	0.0	4.0
	Percentage	80.0	0.0	80.0
24	Total	0.0	1.0	1.0
	Percentage	0.0	20.0	20.0
Grand total	Total	4.0	1.0	5.0
	Percentage	80.0	20.0	100.0

Table 10: Gender of respondent * q5 Cross tabulation

		q5			
Respondent gender	Count	Yes	No	Don't know	Total
Male	Total	20.0	11.0	5.0	36.0
	Percentage	24.4	13.4	6.1	43.9
Female	Total	33.0	9.0	4.0	46.0
	Percentage	40.2	11.0	4.9	56.1
Total	Total	53.0	20.0	9.0	82.0
	Percentage	64.6	24.4	11.0	100.0

However, as shown in Table 11, the majority (58.5%) believed that they would support newly merged companies from internally sharing information about them, while (15.9%) did not care. Table 11 shows that most of the respondents (23.2%) who supported information sharing were of age 22.

Relatively few respondents (2.1%) thought that companies do not have to notify them before sharing their personal financial information with newly affiliated companies. On the other hand, the majority (89.6%) thought that companies have to notify them. These results are clearly demonstrated in Table 12.

Table 13 shows only (22%) reported that they have experienced a case where a company was inappropriately sharing or selling their personal information while (68.3%) have not been in this situation. Of the (22%), only (8.5%) were females while the rest (13.4%) were males.

Table 11: Age of respondent * q6 Cross tabulation

		q6				
Age of respondent		Support	Oppose	Don't care	Don't know	Total
21	Total	14.0	2.0	5.0	0.0	21.0
	Percentage	17.1	2.4	6.1	0.0	25.6
22	Total	19.0	0.0	4.0	10.0	33.0
	Percentage	23.2	0.0	4.9	12.2	40.2
23	Total	2.0	0.0	4.0	3.0	9.0
	Percentage	2.4	0.0	4.9	3.7	11.0
24	Total	11.0	0.0	0.0	0.0	11.0
	Percentage	13.4	0.0	0.0	0.0	13.4
25	Total	2.0	4.0	0.0	2.0	8.0
	Percentage	2.4	4.9	0.0	2.4	9.8
Grand total	Total	48.0	6.0	13.0	15.0	82.0
	Percentage	58.5	7.3	15.9	18.3	100.0

Table 12: Age of respondent * q7 Cross tabulation

		q7			
Age of respondent	Count	Yes	No	Don't know	Total
21	Total	14.0	0.0	0.0	14.0
	Percentage	29.2	0.0	0.0	29.2
22	Total	17.0	0.0	2.0	19.0
	Percentage	35.4	0.0	4.2	39.6
23	Total	2.0	0.0	0.0	2.0
	Percentage	4.2	0.0	0.0	4.2
24	Total	10.0	1.0	0.0	11.0
	Percentage	20.8	2.1	0.0	22.9
25	Total	0.0	0.0	2.0	2.0
	Percentage	0.0	0.0	4.2	4.2
Grand total	Total	43.0	1.0	4.0	48.0
	Percentage	89.6	2.1	8.3	100.0

Table 13: Gender of respondent * q5 Cross tabulation

		q8			
Respondent gender	Count	Yes	No	Don't know	Total
Male	Total	11.0	25.0	0.0	36.0
	Percentage	13.4	30.5	0.0	43.9
Female	Total	7.0	31.0	8.0	46.0
	Percentage	8.5	37.8	9.8	56.1
Total	Total	18.0	56.0	8.0	82.0
	Percentage	22.0	68.3	9.8	100.0

An interview was held with the IT Support Manager of a telecommunications company, to investigate the role of IS professionals in protecting data privacy and the interview has revealed many vital points. The IT Support Manager believed that privacy concerns are a major issue that must be addressed and that there are few legal constraints on the collection and dissemination of information about individuals. In addition, he pointed out that they might sell personal information to other affiliated companies if customers will benefit from that. The IT Support Manager thought there was no gap in the privacy protections for consumers in the company. However, he believed that existing protections are not strong enough.

CONCLUSIONS

It is getting easier to collect personal data, not because information technology inevitably must provide those capabilities, but rather because government and commercial interests want to track what people are doing and when[6].

The results of this research show the increasing concerns of individuals regarding their personal data privacy. It seems that these concerns are increasing because the current and existing protections are not strongly enough. This research aimed to attract the attentions toward the privacy issues and the role of IS auditors and professionals in protecting individuals' privacy.

In conclusion, it is extremely important to note that IS audit plays the critical role in providing reliable measures that would control the use and access of the huge personal data stored in any organization. In this regard, we should not neglect the responsibility of the government through stating laws and legislations that enforce the privacy rights of individuals.

RECOMMENDATIONS

Careful consideration of the implications of personal information privacy issues should be a priority in organizations. Conscious and deliberate decisions must be made by upper management on the operation, control, and management of information services[1].

Managers should identify any potential underlying privacy-related problems and be prepared to take corrective actions and appropriate measures to protect the individual's privacy. Managers need to be aware of new developments. One person should be designated responsible for information system auditing and to maintain a close connection with functional area managers. This practice would help ensure that privacy policies are maintained and that the information reaches the appropriate personnel. Close contact with the functional area managers would help the designated person keep up with the organization's practices concerning personal information.

Currently, there is a need for IS managers to take a proactive stance regarding information privacy management issues. If they do not do so, levels of concern about information will continue to rise and citizens will look to the government for solutions.

IS managers need to think through potential information problems within their firms and take action to reduce the risk that their information systems might be used to invade an individual's privacy.

There are several areas in which IS managers should be particularly cautious. First, an organization should not store information that it does not need. Second, information should be used for the purposes for which it was collected or for which individuals believe it was collected. Third, if information is shared electronically, the organization should have approval of the individuals concerned or knowledge that the individuals would approve of the sharing. Next, proper human judgment should be used in making decisions concerning an individual's personal information. Auditors and IS professionals should also be cautious when pieces of personal information are pulled from different sources to make a more complete file. Finally, internal controls and procedures should be in place to prevent and/or correct any errors in an individual's personal information.

REFERENCES

1. Henderson, S. and A.S. Charles, 1999. Personal information privacy: Implications for MIS managers. Inform. Manage. [online], http://www.sciencedirect.com [Accessed March 5, 2005], 36: 213-220.
2. Senicar, V., B. Jerman-Blazic and T. Klobucar, 2003. Privacy-enhancing technologies approaches and development. Comp. St. Interf; [online], http://www.sciencedirect.com [Accessed March 6, 2005], 25: 147-158.
3. Hinde, S., 2003. Careless about privacy. Comp. Sec., [online], http://www.sciencedirect.com [Accessed March 5, 2005], 22: 284-288.
4. Weber, R., 1998. Information Systems Control and Audit. 1st Edn., Prentice Hall, pp: 5-10.
5. Sayana, S.A., 2002. IT Audit Basics. Inform. Sys. Control J., [online]. http://www.isaca.org [Accessed May 15, 2005].
6. Shapiro, B. and C.R., Baker, 2001. Information technology and the social construction of information privacy. J. Acc. Pub. Policy [online], http://www.sciencedirect.com [Accessed March 5, 2005], 20: 295-322.