Information Privacy Status in Saudi Arabia

Laith A. Alsulaiman[1] & Waleed A. Alrodhan[1]

[1] College of Computing and Information Sciences, Imam Mohammed Ibn Saud Islamic University, Riyadh, Saudi Arabia

Correspondence: Laith A. Alsulaiman, College of Computing and Information Sciences, Imam Mohammed Ibn Saud Islamic University, Riyadh, Saudi Arabia. Tel: 966-112-258-1818. E-mail: laith@ccis.imamu.edu.sa

Received: July 5, 2014 Accepted: July 21, 2014 Online Published: July 29, 2014

doi:10.5539/cis.v7n3p102 URL: http://dx.doi.org/10.5539/cis.v7n3p102

Abstract

Privacy is one of the most fundamental rights that must be preserved for individuals because it is integral to their integrity, self-respect, and safety. However, it is also a vague concept with a number of controversial issues that need to be addressed from ethical, jurisdictional, and sociological perspectives. The perceptions of both organizations and individuals have undergone noticeable changes since the introduction of communication and processing technologies. Furthermore, with the dominance of the Internet and social networks in business and personal lives, information privacy appears to be a myth as massive volumes of personal information and data are stored in the Cloud and back end systems of organizations. Such systems have created serious legal, ethical, and technological challenges related to information collection, processing, and dissemination. This paper presents the findings of the first phase of a countrywide research project that aims to provide a comprehensive assessment of information privacy practices in the public, health, banking, and private sectors. The results presented in this paper are based on a survey and structured interviews with key stakeholders in multiple organizations in the Kingdom of Saudi Arabia to measure organizational compliance and personal perceptions of information privacy.

Keywords: information privacy, information security, security policies, penetration testing, IT governance, Saudi Arabia

1. Introduction

Privacy is one of the most fundamental rights that must be preserved for individuals because it is integral to their integrity, self-respect, and safety. However, it is also a vague concept that is associated with controversial issues that need to be addressed from ethical, jurisdictional, and sociological perspectives. As technologies advance, new privacy challenges arise owing to the pervasive and ubiquitous availability of information.

Many countries have addressed privacy in their laws and have designed regulations for specific sectors (such as communication, health, and commerce) to preserve information privacy. Additionally, huge efforts have been made to model privacy in computing and to develop proper solutions to map privacy business requirements into user applications and systems.

In this paper, we will present the outcome of the first phase of a 2-year project (Alrodhan & Alsulaiman, 2014) (Alsulaiman & Alrodhan, 2012) that aims to assess and analyze information privacy practices in the Kingdom of Saudi Arabia. The study looks at privacy practices in terms of current regulations, technical controls, perception, and awareness at various sectors. To date, there has been very little research on this issue in Saudi Arabia. The only serious and relevant study to the best of our knowledge is that conducted by the Saudi MCIT (Ministry of Communications and Information Technology) to propose a Law Regulating Electronic Privacy and Data Protection in Saudi Arabia (e-Privacy Act) (MCIT, 2010). However, the study only covers legislation aspects and does not address how privacy is perceived nor how the current regulations are implemented in organizations.

We followed four strategies for the assessment; namely, an online survey, structured interviews, penetration testing, and social engineering. The results were insightful and will be presented later in the paper.

The remainder of the paper is organized as follows. Section 2 describes the assessment approach and methodology. Section 3 discusses our findings and recommendations. Section 4 presents concluding remarks and potential future work.

1.1 Overview of Privacy

There have been many attempts to define privacy and many philosophers, jurists, sociologists, and even computer scientists, have created definitions based on their context. However, most of those definitions have shortcomings (Solove, 2008). An excellent comprehensive definition of privacy is "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated" (Westin, 1967). In a computing context, privacy is an information security service that protects the attributes, preferences, and traits associated with individuals' identities against unauthorized distribution or use (Windley, 2005).

Figure 1 shows an expanded and slightly different representation of the classic three-phase information lifecycle diagram (input, process, and output). In the information collection phase, relevant private data could be collected from individuals (or data subjects) by an organization (also known as data controller) that then uses this data to make decisions. Typically, data is processed in-house or outsourced to the IT department (also known as the data processor), making personal data subject to various privacy invasion attacks.

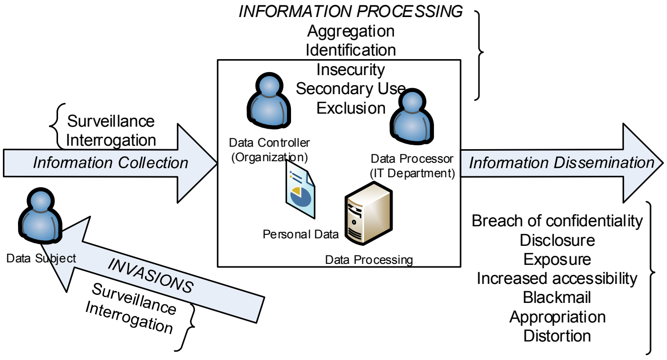


Figure 1. Data protection and privacy taxonomy (adopted from (Solove, 2008))

The protection of private information (i.e., personal data) against unauthorized disclosure must be considered as a 'right' of individuals (i.e., data subjects). Information, be it medical, criminal, biological, ethnicity, or political, can negatively impact the data subject when unauthorized disclosure occurs by the data controller that holds the personal data. For example, disclosing medical records might impact on insurance coverage, employment, or one's social life. Table 1 presents a good categorization of possible privacy problems that could occur at each stage of the information lifecycle.

Table 1. Taxonomy of privacy problems adopted from (Solove, 2008) framework

Stage	Possible Problem	Definition
Information collection	Surveillance	Watching, recording and capturing of data subject's activities
	Interrogation	Activity questioning or probing for information
Information processing	Aggregation	Combining various pieces of information about the data subject
	Identification	Linking information to particular data subject
	Insecurity	Data controller not taking sufficient measurements to protect data subject information from leaks or misuse
	Secondary use	Using collected information to purpose other that what has been stated
	Exclusion	Not allowing data subjects to know about what has been collected about them and provide them the ability to correct inaccurate information
Information dissemination	Breach of confidentiality	Breaking the trust between the data subject and data controller in keeping confidential data
	Disclosure	Revealing truthful information which data subject's that

		affects their reputation
	Exposure	Revealing data subjects body, grief, or nudity (not data)
	Increased accessibility	Amplifying the accessibility of information by data controller without proper justifications
	Blackmail	Threating data subject to disclose personal information
	Appropriation	Using data subject identity to serves another another's interests.
	Distortion	Disseminating false or inaccurate information about data subject
Invasion	Intrusion	Invasion of person life and distrusting victim's daily activities or routines (e.g. junk mail, telemarking…)
	Decisional interference	Intruding into the data subject's decisions (to change it)

1.2 Privacy Regulations and Standards

1.2.1 International Overview

Privacy issues have captured the attention of many countries around the world. Many nations have addressed privacy at various levels, starting from the constitution that protects privacy as a basic human right and going further to set specific laws and technical requirements for information privacy. For example, the Brazilian constitution states, "the privacy, private life, honor and image of persons are inviolable" (The Constitution of Brazil, 2013). Canada has the Personal Information Protection and Electronic Documents Act 2000 (The Office of The Commissioner of Canada, 2000) and Japan the Personal Information Protection and Electronic Documents Law of 2003 (The Government of Japan, 2003). Both laws address how personal information shall be collected, processed, and disseminated by government agencies and private entities.

The relevant U.K. laws include the following laws: (Data Protection Act , 1998); (The Freedom of Information Act, 2000); (The Environmental Information Regulations, 2004); and (The Privacy and Electronic Communications (EC Directive) Regulations, 2003).

In the United States, privacy protection has been addressed in hundreds of sector specific state and federal laws. For example, (The Health Insurance Portability and Accountability Act, 1996) establishes security and privacy rules that specify various administrative, physical, and technical controls to assure the confidentiality, integrity, and availability of electronic health information related to individuals. Other laws include (The Privacy Act, USA , 1974), (The Children's Online Privacy Protection Act, 1998), and (The Financial Services Modernization Act, 1999).

Furthermore, there have been multinational efforts to establish privacy guidelines and frameworks such as the one created by the (OECD, 1980), the European Union's directive on data protection in 1995, and the APEC framework (ECSG, 2005).

1.2.2 Information Privacy in Saudi Arabia

Currently, there is no specific law in the Kingdom of Saudi Arabia that targets information privacy, with the exception of some provisions and articles scattered in various regulations, such as those in (Royal decree , 1992) (CITC, 2001) (MCIT, 2007) (CITC, 2007). For example, Article 40 of the Basic Law of Government states "The privacy of telegraphic and postal communications, and telephone and other means of communication shall be inviolate. There shall be no confiscation, delay, surveillance or eavesdropping, except in cases provided by the Law" (Royal decree, 1992). The Telecom Act (CITC, 2007) is more specific in protecting information exchanged through public networks. However, in 2010, the Saudi Ministry of Communications and Information Technology (MCIT) adopted an initiative and proposed an e-Privacy law to have a unified general law that addresses issues related to information privacy, similar to that practiced by other countries, and to support MCIT Plan goals (MCIT, 2010). The proposed law adopts many principles stated in the (The Madrid Resolution: International Standards on the Protection of Personal Data and Privacy, 2009) and the APEC Privacy Framework (ECSG, 2005) such as the right for a person to be notified before the collection of his/her personal information. The law was proposed to take precedence and preempt contrary laws and regulations unless they provide more protection for information privacy. Unfortunately, the Shura Council, under the belief that the existing cybercrime law (MCIT, 2007) is sufficient, has rejected the proposed law. In our opinion, the proposed law has many advantages as it provides consolidated and structured privacy principles that can be implemented in all governmental and business sectors.

1.3 Addressing Privacy in Computing

Privacy has been addressed in many contexts from formal protection modeling of privacy to ensure anonymity and to the design of applications and protocols that address specific threats (Sweeney, k-anonymity: A model for protecting privacy, 2002). For example, the TOR Project aims to protect privacy and guarantee anonymity by implementing an encrypted network overlay on the Internet using the Onion Routing Protocol (Dingledine, Mathewson, & Syverson, 2004). Another tool is the Private Web Search (Saint-Jean, Johnson, Boneh, & Feigen, 2007), a browser extension that aims to minimize private information that could be revealed by intercepting queries sent to search engines that may identify data subjects (e.g., SSN info and phone numbers). Other multidisciplinary projects such as PORTIA (Privacy, Obligations, and Rights in Technologies of Information Assessment (PORTIA)., 2013), (Sweeney, Shamos, & Madhava, Social Security Number Watch, 2013), Information Accountability (Weitzner, Abelson, Berners-Lee, & Fei, 2008), Ensuring Consent and Revocation (EnCore) (Mont, Sharma, Pearson, Saeed, & Filz, November 2011), and Hippocratic Database (Bolton, 2003) are very good examples where privacy has been addressed from technical, legal, and social perspectives.

In contrast, there are huge efforts in the field of computing to identify and discover security flaws and privacy issues in computer systems at every level, from design to implementation. Many tools have been developed to automate the process of detecting and exploiting vulnerabilities such as (Acuntix, 2013), (Nessus, 2014), (Nikto, 2014), (Nmap, 2013), and (Shodan HQ, n.d.). We have also used these tools to support our thesis and to demonstrate how easy it is to extract private data.

2. Assessment Methodology

This section shows the approach we followed for our privacy assessment:

a) Review of relevant regulations in Saudi

b) Field survey

c) Structured interviews

d) Penetration testing and social engineering

The following subsections highlight each method.

2.1 Review of Relevant Regulations in Saudi

We examined the majority of publicly available key legislation and regulations for each sector in the Kingdom and extracted every provision related to data collection and dissemination, with an emphasis on the five sectors mentioned earlier. Our interest in the regulation review is to identify if privacy is addressed and to classify what privacy problems they tackle as presented in Table 1. The analysis should not be treated as a legal assessment because that is beyond the scope of this research. Instead, we attempted to identify how such regulations can be mapped into information security management systems and controls (i.e., technical, physical, and/or administrative) as this is a very important step in terms of the future work of the project.

2.2 Field Survey

The objective of the survey was to evaluate information privacy perceptions and adherence in a sample of professional workers and decision makers representing government, education, health, banking, and business sectors (Note 1). The survey was distributed electronically, as well as hardcopies, and we received a relatively good number of responses: 101 in total including 34 responses from decision makers distributed in terms of demographics as shown in Table 2. The survey's questions measure the following metrics:

1) Existence and adherence of information privacy policies and practices at the organization level.

2) Awareness and perception of privacy issues related to clients, employees, and citizens.

For decision makers, there were additional questions to verify organizations' maturity in taking due care and due diligence measurements on information privacy and data protection.

Table 2. Demographic attributes of the responses

	Female			*Male*				
	Bachelor	Masters	Ph.D.	Bachelor	High School	Masters	Ph.D.	Grand Total
Education	**5**		**1**	**10**	**2**	**3**	**10**	**31**
2-5 years	1			2		2	5	10
Less than 2 years	2		1	7	1		1	12
More than five years	2			1	1	1	4	9
Finance/Banking	**2**			**9**		**1**		**12**
2-5 years				2				2
Less than 2 years				1				1
More than five years	2			6		1		9
Governmental Services	**4**	**1**		**13**	**4**	**3**		**25**
2-5 years	4	1		2	1			8
Less than 2 years				7		1		8
More than five years				4	3	2		9
Health				**7**		**7**	**6**	**20**
2-5 years				2		2	1	5
Less than 2 years				3				3
More than five years				2		5	5	12
Industry				**5**		**6**	**2**	**13**
2-5 years						2		2
Less than 2 years				2				2
More than five years				3		4	2	9
Grand Total	11	1	1	44	6	20	18	101

2.3 Structured Interviews

We conducted personal interviews with a number of key stakeholders in major organizations representing Telco, health, banking, government, and educational sectors. The interviewed stakeholders were responsible for managing information technology and the information security department for their organization. The purpose of the interview was to cross-check the survey findings and to reveal more detailed information regarding information privacy practices, in addition to evaluating organizations' adherence against the applicable privacy requirements and principles mentioned in (MCIT, 2010) and (CITC, 2001) (e.g., the right of the data subject to access his/her information and data retention for personal data).

2.4 Penetration Testing and Social Engineering

The last approach we used in this study was to perform penetration testing after obtaining official consent from the organizations' authorities. The objective was to verify whether we could obtain what is usually considered private information (e.g., customers, citizens). Our approach was to select sample organizations that represent educational and telecommunications sectors. We then navigated through publicly available information on the website using basic technology tools (see Table 3), without interrupting the service to identify potential vulnerabilities.

Table 3. Tools used to conduct penetration testing

#	Tool Name	Description
1	Nessus	Popular open source vulnerability scanner
2	Nikto	Open source web vulnerability scanner
3	Acuntix	Commercial, web vulnerability scanner
4	Nmap	Network scanning engine
5	Shodan HQ	Web information revealing and passive scanning site.

3. Results Discussion and Recommendations

3.1 Regulations Review Findings

Table 4 summarizes our findings for the reviewed regulations; please notice that the table only shows regulations that have articles or clauses related to information security and privacy, which, of course, is a subset of what has been reviewed. The first two columns present the regulation title and relevant article(s). The third column presents the privacy issues or problems it addresses. For example, in the Anti-Cyber Crime Law, Article 3 criminalizes any person who commits one of the following cybercrimes: “1) Spying on, interception or reception of data transmitted through an information network or a computer without legitimate authorization. 2) Unlawful access to computers with the intention to threaten or blackmail any person to compel him to take or refrain from taking an action be it lawful or unlawful. 3) Unlawful access to a web site, or hacking a web site with the intention to change its design, destroy or modify it, or occupy its URL. 4) Invasion of privacy through the misuse of camera-equipped mobile phones and the like. 5) Defamation and infliction of damage upon others through the use of various information technology devices” (MCIT, 2007). From that article, we can determine that surveillance, intrusion, blackmailing, distortion, exposure, and disclosure privacy issues were addressed.

Table 4. List of privacy-related articles in reviewed laws and regulations

Regulation name	Information Privacy Related Clause	Addressed Privacy Problem
The Basic Law of Government (Royal decree , 1992)	Article 40,	Surveillance, Insecurity, intrusion
Communication Act (CITC, 2001)	Section 10, Article 37, Article 38	Surveillance, Disclosure, Breach of confidentiality, Intrusion
Anti-Cyber Crime Law (MCIT, 2007)	Article 3, Article 4, Article 5	Surveillance, Intrusion, Disclosure, Blackmail, Exposure, Distortion, Decisional interference, Appropriation,
Communication Act (practice statements) (CITC, 2002)	Article 56	Disclosure, Breach of confidentiality, Exclusion, Insecurity,
Income tax law (SAMA, 2004)	Article 95	Insecurity, Breach of confidentiality, Disclosure, Secondary use
e-Government Implementation Rules (Council of Ministers, 2006)	Article 8	Breach of confidentiality, disclosure, insecurity
Computing and networking controls in Government Agencies (Council of Ministers, 2009)	Article 4	Surveillance, Breach of confidentiality, disclosure, insecurity, secondary use, increased accessibility, Appropriation, intrusion, blackmail, distortion,
Rules governing awarding of IT contracts to private sector (the Council of Ministers, 2004)	Article 11	Insecurity
Business rules of Saudi Credit Information	Article 4	Insecurity, Secondary use,

		Exclusion, Breach of confidentiality, Disclosure, Distortion, Aggregation, Identification
Manual of Combating Embezzlement & Financial Fraud & Control Guidelines (SAMA, 2008)	Article 2, 3.	Insecurity, Distortion, Disclosure, Increase accessibility
SAMA's Outsourcing guidelines (SAMA, 2008)	Article 5.3	Insecurity, Disclosure, Breach of confidentiality,
Medical guidelines – rights and responsibilities of patients (MOH, 2012)	Article 3	Disclosure, Breach of confidentiality, Exposure, Distortion, Decisional, Appropriation
Fertilization units, embryos and infertility treatment law (MOH, 2004)	Article 12	Breach of confidentiality, Exposure
Healthcare practitioners law (MOH, 2005)	Article 21	Breach of confidentiality
Cooperative health insurance law practice statements (MOH, 2002)	Article 64	Breach of confidentiality,

From the table above, the regulations in most of the examined sectors do have provisions on information privacy. However, the major concern in our context is that many of them are so broad and require supporting written compliance programs specifically directed at privacy and data security in the respected domains. Unfortunately, we were not able to identify any that are supported by the structured interviews and survey findings. This is important when designing and developing IT systems that need to comply and implement privacy requirements as stated in the relevant regulations. For example, part of our current project is to develop privacy profiles based on XACML (OASIS Open, 2010) for each sector, which maps applicable privacy policies into PEP. This is to ensure that all business applications and systems will adhere to the relevant privacy policy when accessing or exchanging personal information. Regrettably, with the level of abstraction we have owing to the lack of detailed compliance programs and procedures, the resulted XACML profiles will have fewer and more generic privacy rules.

In addition to this finding, there are other observations and shortcomings—most of them are regulatory and detailed in (MCIT, 2010).

3.2 Survey Analysis

The survey feedback revealed very insightful information with respect to privacy status in Saudi. In this section, we list the most important findings and prefer to place the full details to Appendix A.

1. Roughly 60% of employees have been asked to follow some specific privacy procedure as shown in Table A.1.

2. Health and public sector employees appear to have received more privacy related procedures (75 and 70%, respectively) as presented in Table A.4. However, when it comes to the question of having a privacy policy adopted by the organization, 67% of the responding sample from the banking sector confirmed the existence of such policy. Forty-five percent of the educational sector respondents answered that they do not know if there is a privacy policy in their organization (see Table A.5)

3. In Table A.8 , we can see that people with a higher level of education, regardless of seniority, tend not to trust their organization when it comes to client/customers privacy protection: PhD (26%) vs. high school (50%). This is consistent with their perceptions regarding their personal information held at the organizations they work for: 67% of those with a high school degree trust their personal data compared with 32% who hold a PhD degree (see Table A.12). Gender also had a slight influence in this aspect. Females tend to have greater trust with respect to their own personal information and that of their customers compared with males (Table A.11).

4. Table A.15shows that when it comes to witnessing incidents of privacy violation, responses from people working in financial sectors are higher (42%) than those in the public sector (24%).

5. Regarding accessing unauthorized information without permission, 34% of the sample had knowledge of such acts regardless of their seniority; however, those in education and finance scored higher (43%) than

the sample average (Table A.16 ,Table A.18 , and Table A.19 , respectively), and only 25% reported the incident. Surprisingly, none of the participants from the financial sector reported such incidents.

6. Thirty-one percent of participants confirmed that their organizations log privacy related issues in their operations. The financial sector seems to be more stringent in that regard (50%) with the education sector scoring the lowest value (19%) (Table A.20).
7. Eighty-four percent of participants believe that privacy protection is important regardless of their seniority as presented in Table A.23. However, just 50% of participants with high school education think that way (Table A.22) compared with 100 and 90% of respondents in the financial and health sectors, respectively (Table A.24).
8. Approximately 50% of participants were unaware of IT criminal laws in Saudi regardless of their education level (Table A.26). Decision makers scored slightly higher (60%) compared with the remainder of the sample (Table A.29).
9. Interestingly, 85% of participants are not satisfied with current status of privacy protection in Saudi, especially those who work in the financial sector as shown in Table A.33.
10. Twenty-six percent of the decision-maker group believes that their organization adheres to a global standard of privacy protection (Table A.35). However, 15% used technical mechanisms for privacy protection (Table A.36).
11. Twenty-seven percent of the decision makers stated that their organizations have privacy officers (Table A.37).
12. With respect to organization seriousness, Table A.38 shows that 32% of the participants believe that their organizations take stakeholders data seriously, especially the financial sector (50%). Participants from the education sector believe their organizations are somewhat serious (50%).
13. Table A.39 shows that 26% of the decision makers answered that their organization audits privacy relevant operations and 42% among them do so once a year.
14. Forty-one percent of the decision makers answered that their organization has a data calcification policy (Table A.41).
15. Table A.42, shows that 18% of the decision makers stated that their organizations encrypt their data, 56% use partial encryption and just 26% do none at all.
16. Thirty-eight percent of decision makers answered that their organizations use a need-to-know basis when allowing access to personal data (Table A.44).
17. Thirty-two percent of decision makers answered that their organizations are subject to international mandates related to data protection as shown in Table A.45.
18. Eighty-two percent believe, as presented in Table A.47, that they are morally obliged to preserve the data of their stakeholders, which indicates that privacy, as a principle, is still perceived as an important human value.

3.3 Structured Interview Feedback

The interview results showed clear gaps and differences in the knowledge, experience, determination, and seriousness in terms of protecting information privacy. However, the sole similarity amongst all the surveyed organizations is that most efforts towards protecting information privacy are somewhat "voluntary". Furthermore, the adopted procedures are selected based on the discretion of the organization rather than from direct mandates issued by regulation and compliance authorities.

To clarify this point, we wish to provide two examples representing two extremes as gleaned from the participants. The first is the information and privacy director of a major telecommunication and Internet service provider in Saudi (CIO, 2013). The second example is an interview conducted with the CIO of a Saudi university under the Ministry of Higher Education (Manager, 2012). The objective of the interview was to determine how decision makers from the selected samples of the organizations working in Saudi address privacy.

The first interview outcome can be summarized into the following points.

1. User data are segregated from all other data; it is not easy to transfer user data between departments from technical and procedural perspectives.
2. Additionally, there was an ongoing pilot implementation of Data Leakage Prevention (DLP) solution to

protect company's information assets, which is a good initiative to reduce the amount of disclosed data.

3. As geographical information is logged by mobile operators for various technical reasons, this information is sensitive and creates privacy concerns in many countries. The company does have special procedures to reveal geographical info and only two people are authorized to disclose such information to law enforcements liaisons.
4. He is not sure if his company sells customer data to third parties, as this is a responsibility of another department.
5. The privacy protection and measurements taken by the company falls under their internal interest to follow best practices and was not mandated by regulators (e.g., the Commission of Information Technology and Communications) or as a response to any international mandate.
6. The organization has a 1-year data retention period for data as they are ISO27001 certified but the choice to do so was irrelevant of any national regulation.
7. In the information security department, there is an ongoing effort to follow international trends in information privacy and they encouraged their team to obtain certification from the International Association of Privacy Professionals (IAPP).

In contrast, the second interview with the CIO of an educational organization shows the opposite in terms of privacy protection as summarized below.

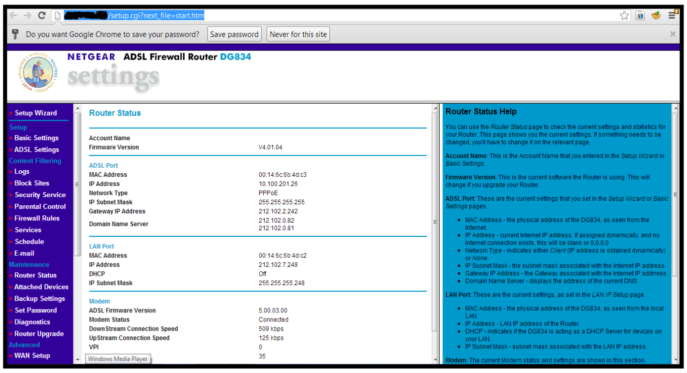
1. Most users' data, mainly students, are not segregated nor encrypted.
2. There are no clear boundaries on what data can be accessed from each department and many times departments have access to classified data without legitimate reasons.
3. There is no information security department, and security controls are ad-hoc and based on the best efforts of IT members.
4. The organization does not implement any ISMS (e.g. ISO27001).

3.4 Penetration Results and Discussion

Penetration testing revealed shocking results, as we were able to demonstrate how easy it is to access and collect private data using very simple on-the-shelf tools as mentioned in Table 3.

We have summarized the findings into the following points.

1. We found many unprotected WIMAX/WIFI CPEs terminals. For example, in two of the tested telecommunication organizations, it was possible to login into users' Internet devices with administrator privileges using a default username and password as shown in Figure 2. This provides the ability for an intruder to intercept and collect all public and private data with a basic update of the routing table of the network device.
2. We found some open webcam servers with default admin/admin passwords with no authentication.
3. Links to firewall configuration GUI's, with NO SSL for authentication.
4. Multiple open anonymous FTP servers.



[redacted]/setup.cgi?next_file=start.htm

Do you want Google Chrome to save your password?

Router Status

Account Name	
Firmware Version	V4.01.04
ADSL Port	
MAC Address	00:14:6c:6b:4d:c3
IP Address	10.100.201.26
Network Type	PPPoE
IP Subnet Mask	255.255.255.255
Gateway IP Address	212.102.2.242
Domain Name Server	212.102.0.82 212.102.0.81
LAN Port	
MAC Address	00:14:6c:6b:4d:c2
IP Address	212.102.7.249
DHCP	Off
IP Subnet Mask	255.255.255.248
Modem	
ADSL Firmware Version	5.00.03.00
Modem Status	Connected
DownStream Connection Speed	509 kbps
UpStream Connection Speed	125 kbps
VPI	0
	35

Router Status Help

You can use the *Router Status* page to check the current settings and statistics for your Router. This page shows you the current settings. If something needs to be changed, you'll have to change it on the relevant page.

Account Name: This is the Account Name that you entered in the *Setup Wizard* or *Basic Settings*.

Firmware Version: This is the current software the Router is using. This will change if you upgrade your Router.

ADSL Port: These are the current settings that you set in the *Setup Wizard* or *Basic Settings* pages.

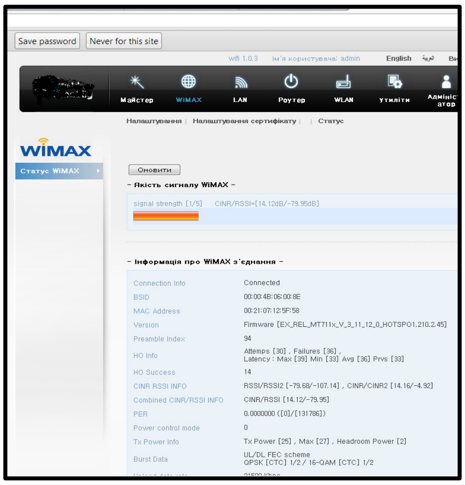
- MAC Address - the physical address of the DG834, as seen from the Internet.
- IP Address - current Internet IP address. If assigned dynamically, and no Internet connection exists, this will be blank or 0.0.0.0
- Network Type - indicates either *Client* (IP address is obtained dynamically) or *None*.
- IP Subnet Mask - the subnet mask associated with the Internet IP address.
- Gateway IP Address - the Gateway associated with the Internet IP addrress.
- Domain Name Server - displays the address of the current DNS.

LAN Port: These are the current settings, as set in the *LAN IP Setup* page.

- MAC Address - the physical address of the DG834, as seen from the local LAN.
- IP Address - LAN IP address of the Router.
- DHCP - indicates if the DG834 is acting as a DHCP Server for devices on your LAN.
- IP Subnet Mask - subnet mask associated with the LAN IP address.

Modem: The current Modem status and settings are shown in this section.

Figure 2. The screenshot represents how easy it is to gain root access to customer-premises equipment (CPE); in this figure the ADSL firewall was accessed



- Якість сигналу WiMAX -

signal strength [1/5] CINR/RSSI=[14.12dB/-79.95dB]

- Інформація про WiMAX з'єднання -

Connection Info	Connected
BSID	00:00:4B:06:00:8E
MAC Address	00:21:07:12:5F:58
Version	Firmware [EX_REL_MT711x_V_3_11_12_0_HOTSPO1.210.2.45]
Preamble Index	94
HO Info	Attemps [30] , Failures [36] , Latency : Max [39] Min [33] Avg [36] Prvs [33]
HO Success	14
CINR RSSI INFO	RSSI/RSSI2 [-79.68/-107.14] , CINR/CINR2 [14.16/-4.92]
Combined CINR/RSSI INFO	CINR/RSSI [14.12/-79.95]
PER	0.0000000 ([0]/[131786])
Power control mode	0
Tx Power Info	Tx Power [25] , Max [27] , Headroom Power [2]
Burst Data	UL/DL FEC scheme QPSK [CTC] 1/2 / 16-QAM [CTC] 1/2

Figure 3. The screenshot represents how easy it is to gain root access to customer-premises equipment (CPE); in this figure the WiMax router was accessed

4. Concluding Remarks and Future Work

In this paper, we presented the current information privacy situation and its challenges in Saudi Arabia by reviewing existing regulations, conducting a countrywide survey, performing interviews with stakeholders, and conducting penetration testing to express our concerns.

We believe that additional efforts are required to close identified gaps in handling information privacy issues in Saudi. We propose that relevant governmental bodies need to create information privacy compliance programs and mandate their implementation in all related entities. Moreover, it is crucial to create a privacy officer function, especially in large organizations, typically within the information security department with the authority to implement privacy compliance programs. Country level awareness initiatives are also needed to create the appropriate perceptions of information privacy and its importance from human rights and consumer standpoints.

For future research, we will focus on the development of XACML profiles and templates, which will be developed based on the privacy rules identified in Table 4. In addition to business applications, these rules will be used by Policy Enforcement Points (or PEPs) such as files servers, mail servers, and firewalls.

We will also participate in the development of compliance frameworks that address privacy, especially in the telecommunications sector.

Acknowledgements

This work was funded by King Abdulaziz City for Science and Technology (KACST) through the Comprehensive Long-Term National Plan for Science, Technology, and Innovation program. Grant 11-INF1896-08

We thank Dr. Abdullah Altamim for his valuable feedback and support, Mr. Mohammed Alhamdan for executing the survey and obtaining relevant regulations, and Mr. Osama Alomari for conducting the penetration testing. We also thank all the anonymous and named participants who provided their feedback during data gathering stage.

References

Acuntix. (2013). *Acuntix*. Retrieved from http://www.acunetix.com.

Agrawal, R., Kiernan, J., Srikant, R., & Xu, Y. (2002). Hippocratic databases. *VLDB*, 143-154.

Alrodhan, W., & Alsulaiman, L. (2014). Information Privacy in Saudi: A Country-Wide Project. *World Symposium on Computer Applications & Research (WSCAR' 2014)*. Sousse, Tunisia.

Alsulaiman, L., & Alrodhan, W. (2012). *Information Privacy in Saudi: Investigation, Assessment, and Solutions.* KACST, ADVANCED AND STRATEGIC TECHNOLOGIES PROGRAM, Riyadh.

Bolton, J. B. (2003). *E-authentication guidance for federal agencies. M-04-04.* Office of Management and Budget, Executive Office of the President, Washington, DC. Retrieved from http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf

CIO. (2013, April 17). *Private interview with chief security officer at Telco provider*. (L. Alsulaiman, Interviewer)

CITC. (2001, June). The Telecom Act. Kingdom of Saudi Arabia: Communications and Information Technology Commission.

CITC. (2002, July 27). *Implementing Regulations of the Telecommunications Law.* Riyadh: Communications and Information Technology.

CITC. (2007). *Anti-SPAM Policy Framework*. Riyadh, Kingdom of Saudi Arabia: Communications and Information Technology Commission.

Council of Ministers. (2006, March 27). E-Government Implementation Rules.

Council of Ministers. (2009). *Computing and networking controls in Government Agencies*. Riyadh. Retrieved from https://www.yesser.gov.sa/en/MechanismsandRegulations/Regulations/Pages/control_computer_information_network-.aspx

Data Protection Act. (1998, July). UK.

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The second- generation onion router. *USENIX Security Symposium* (pp. 303-320). Retrieved from http://dl.acm.org/citation.cfm?id=1251375.1251396

ECSG. (2005). APEC Privacy Framework. APEC: Electronic Commerce Steering Group.

Manager, I. (2012, December 15). Interview with IT manager at a Sauid University. (L. Alsulaiman, Interviewer) Riyadh.

MCIT. (2007, March). *Anti-Cyber Crime Law*. Kingdom of Saudi Arabia: Bureau of Experts at the Council of Ministers.

MCIT. (2010). *Proposed Law Regulating Electronic Privacy and Data Protection in Saudi Arabia (e-Privacy Act): Public Consultation Request.* Riyadh.

Ministry of Health (Saudi Arabia). (n.d.). *cooperative health insurance law*. Retrieved from http://www.moh.gov.sa/Ministry/Rules/Documents/007.pdf

MOH. (2002). *Cooperative health insurance law practice statements*. Retrieved from http://www.moh.gov.sa/Ministry/Rules/Documents/003.pdf

MOH. (2004). *Fertilization units, embryos and infertility treatment law*. Retrieved from http://www.moh.gov.sa/Ministry/Rules/Documents/014.pdf

MOH. (2005). *Healthcare practitionars law*. Retrieved from http://www.moh.gov.sa/Ministry/Rules/Documents/013.pdf

MOH. (2012). *Medical guidelines – rights and responsibilities of patients*. Retrieved from http://www.moh.gov.sa/HealthAwareness/EducationalContent/HealthInstructions/Pages/001.aspx

Mont, M. C., Thyne, R., & Bramhall, P. (2005). *Privacy enforcement with HP select access for regulatory compliance.* HP Laboratories, Bristol, UK. Retrieved from http://www.hpl.hp.com/techreports/2005/HPL-2005-10.pdf

Mont, M. C., Sharma, V., Pearson, S., Saeed, R., & Filz, M. (November 2011). *Technical Architecture arising from the third Case Study.* EnCore Project.

Nessus. (2014). Retrieved from http://en.wikipedia.org/wiki/Nessus_(software)

Nikto. (2014). Retrieved from http://en.wikipedia.org/wiki/Nikto_Web_Scanner

Nmap. (2013). Retrieved from http://en.wikipedia.org/wiki/Nmap

OASIS Open. (2010, August). *eXtensible Access Control Markup Language (XACML) Version 3.0.* OASIS Standard Specification. Retrieved from http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html

OASIS Open. (2010). *XACML v3.0 Privacy Policy Profile Version 1.0.* OASIS Standard Specification. Retrieved from http://docs.oasis-open.org/xacml/3.0/xacml-3.0-privacy-v1-spec-cd-03-en.pdf

OECD. (1980, September). OECD guidelines on the protection of privacy and trans border flows of personal data. Organization for Economic Co-operation and Development.

Privacy, Obligations, and Rights in Technologies of Information Assessment (PORTIA). (2013, December 16). Retrieved from http://crypto.stanford.edu/portia

Royal decree. (1992, March). The Basic Law of Government Kingdom of Saudi Arabia. Saudi Arabia: Majlis Ash-Shura.

Saint-Jean, F., Johnson, A., Boneh, D., & Feigen, J. (2007). Private web search. *WPES,* 84–90. http://dx.doi.org/10.1145/1314333.1314351

SAMA. (2004, March 6). Income Tax Law. Royal Decree No. M/1 15/1/1425H.

SAMA. (2008). *Manual of Combating Embezzlement & Financial Fraud & Control Guideline.*

SAMA. (2008, July 19). Rules on Outsourcing. *(16/7/1429H).*

Shodan HQ. (n.d.). Retrieved from http://en.wikipedia.org/wiki/Shodan_

Solove, D. J. (2008). *Understanding Privacy.* Cambridge, Massachusetts: Harvard University Press. http://dx.doi.org/10.3366/elr.2010.0323

Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 10*(5), 557-570. http://dx.doi.org/10.1142/S0218488502001648

Sweeney, L., Shamos, M., & Madhava, K. (2013, Dec). *Social Security Number Watch*. Retrieved from http://dataprivacylab.org/projects/ssnwatch

The Children’s Online Privacy Protection Act. (1998). USA.

The Constitution of Brazil. (2013, December 16). Retrieved from http://www.v- brazil.com/government/laws/constitution.html

the Council of Ministers. (2004, June). Rules governing awarding of IT contracts to private sector. Riyadh. Retrieved from https://www.yesser.gov.sa/en/MechanismsandRegulations/Regulations/Pages/rules_governing_private_sector_participation.aspx

The Environmental Information Regulations. (2004). UK.

The Financial Services Modernization Act. (1999). USA.

The Freedom of Information Act. (2000). UK.

The Government of Japan. (2003). Act on the Protection of Personal Information.

The Health Insurance Portability and Accountability Act. (1996). USA.

The Madrid Resolution: International Standards on the Protection of Personal Data and Privacy. (2009). *International Conference of Data Protection and Privacy Commissioners.* Madrid, Spain.

The Office of The Commissioner of Canada. (2000). The Personal Information Protection and Electronic Documents Act. Canada.

The Privacy Act, USA . (1974).

The Privacy and Electronic Communications (EC Directive) Regulations. (2003). UK.

Weitzner, D. J., Abelson, H., Berners-Lee, T., & Fei, J. (2008). Information accountability. *Communication ACM, 51*(6), 82–87. http://dx.doi.org/10.1145/1349026.1349043

Westin, A. (1967). *Privacy and freedom.* Scribner.

Windley, P. (2005). *Digital Identity.* O’Reilly Media.

Note

Note 1. The defense and law enforcement sectors were excluded from our survey because it is difficult to obtain official and reliable data owing to the sensitive nature of those sectors.

Appendix A

Survey Questionnaires and Feedback

This appendix contains survey questionnaires and results in tabular format (A.1 was completed by all participants and A.2 was addressed for decision makers only)

A.1 Survey Questionnaires for All Participants

A.1.1 Have you been asked to follow specific 'privacy-protection' procedures (and/or regulations) that should protect the privacy of your organization's clients/customers/users?

Table A.1. Results of survey question A.1.1 grouped by gender

	No	*Yes*	*Grand Total*
Female	46.15%	53.85%	100%
Male	38.64%	61.36%	100%
Grand Total	39.60%	60.40%	100%

Table A.2. Results of question A.1.1 grouped by education level

	No	*Yes*	**Grand Total**
Bachelor	40.00%	60.00%	100%
High School	16.67%	83.33%	100%
Masters	28.57%	71.43%	100%
Ph.D.	57.89%	42.11%	100%
Grand Total	39.60%	60.40%	100%

Table A.3. Results of question A.1.1 grouped by years of experience

	No	*Yes*	**Grand Total**
2-5 years	44.44%	55.56%	100%
Less than 2 years	42.31%	57.69%	100%
More than five years	35.42%	64.58%	100%
Grand Total	39.60%	60.40%	100%

Table A.4. Results of question A.1.1 grouped by industry

	No	*Yes*	**Grand Total**
Education	58.06%	41.94%	100%
Finance/Banking	41.67%	58.33%	100%
Public sector	32.00%	68.00%	100%
Health	30.00%	70.00%	100%
Others	23.08%	76.92%	100%
Grand Total	39.60%	60.40%	100%

A.1.2 Has a formal 'privacy policy' been deployed in your organization?

Table A.5. Results of question A.1.2 grouped by industry

	I do not know	*No*	*Yes*	**Grand Total**
Education	45.16%	29.03%	25.81%	100%
Finance/Banking	0.00%	33.33%	66.67%	100%
Public sector	24.00%	32.00%	44.00%	100%
Health	15.00%	35.00%	50.00%	100%
Others	0.00%	38.46%	61.54%	100%
Grand Total	22.77%	32.67%	44.55%	100%

Table A.6. Results of question A.1.2 grouped by industry

If you marked "yes", have you read it?				
	NA	No	Yes	Grand Total
Education	58.06%	32.26%	9.68%	100%
Finance/Banking	41.67%	8.33%	50.00%	100%
Public sector	28.00%	20.00%	52.00%	100%
Health	65.00%	15.00%	20.00%	100%
Others	30.77%	23.08%	46.15%	100%
Grand Total	46.53%	21.78%	31.68%	100%

A.1.3 Do you think that private information that belongs to your organization's clients/customers/users is properly protected?

Table A.7. Results of question A.1.3 grouped by gender

	I do not know	*No*	*Yes*	**Grand Total**
Female	30.77%	23.08%	46.15%	100%
Male	23.86%	38.64%	37.50%	100%
Grand Total	24.75%	36.63%	38.61%	100%

Table A.8. Results of question A.1.3 grouped by education level

	I do not know	*No*	*Yes*	**Grand Total**
Bachelor	25.45%	30.91%	43.64%	100%
High School	33.33%	16.67%	50.00%	100%
Masters	19.05%	47.62%	33.33%	100%
Ph.D.	26.32%	47.37%	26.32%	100%
Grand Total	24.75%	36.63%	38.61%	100%

Table A.9. Results of question A.1.3 grouped by years of experience

	I do not know	*No*	*Yes*	**Grand Total**
2-5 years	29.63%	37.04%	33.33%	100%
Less than 2 years	23.08%	34.62%	42.31%	100%
More than five years	22.92%	37.50%	39.58%	100%
Grand Total	24.75%	36.63%	38.61%	100%

Table A.10. Results of question A.1.3 grouped by industry

	I do not know	*No*	*Yes*	**Grand Total**
Education	25.81%	41.94%	32.26%	100%
Finance/Banking	25.00%	50.00%	25.00%	100%
Public sector	24.00%	24.00%	52.00%	100%
Health	40.00%	35.00%	25.00%	100%
Others	0.00%	38.46%	61.54%	100%
Grand Total	24.75%	36.63%	38.61%	100%

A.1.4 Do you think that 'your' private information held by your organization is properly protected?

Table A.11. Results of question A.1.4 grouped by gender

	I do not know	*No*	*Yes*	**Grand Total**
Female	23.08%	23.08%	53.85%	100%
Male	18.18%	37.50%	44.32%	100%
Grand Total	18.81%	35.64%	45.54%	100%

Table A.12. Results of question A.1.4 grouped by education level

	I do not know	*No*	*Yes*	**Grand Total**
Bachelor	21.82%	29.09%	49.09%	100%
High School	16.67%	16.67%	66.67%	100%
Masters	14.29%	42.86%	42.86%	100%
Ph.D.	15.79%	52.63%	31.58%	100%
Grand Total	18.81%	35.64%	45.54%	100%

Table A.13. Results of question A.1.4 grouped by years of experience

	I do not know	*No*	*Yes*	**Grand Total**
2-5 years	18.52%	40.74%	40.74%	100%
Less than 2 years	19.23%	30.77%	50.00%	100%
More than five years	18.75%	35.42%	45.83%	100%
Grand Total	18.81%	35.64%	45.54%	100%

Table A.14. Results of question A.1.4 grouped by industry

	I do not know	*No*	*Yes*	**Grand Total**
Education	19.35%	48.39%	32.26%	100%
Finance/Banking	25.00%	33.33%	41.67%	100%
Public sector	12.00%	28.00%	60.00%	100%
Health	30.00%	25.00%	45.00%	100%
Others	7.69%	38.46%	53.85%	100%
Grand Total	18.81%	35.64%	45.54%	100%

A.1.5 Have you come across a privacy-violation incident within your workplace?

Table A.15. Results of question A.1.5 grouped by industry

	I do not know	*No*	*Yes*	**Grand Total**
Education	6.45%	54.84%	38.71%	100%
Finance/Banking	8.33%	50.00%	41.67%	100%
Public sector	24.00%	52.00%	24.00%	100%
Health	0.00%	70.00%	30.00%	100%
Others	0.00%	61.54%	38.46%	100%
Grand Total	8.91%	57.43%	33.66%	100%

A.1.6 Do you (or any of your colleagues) have access to private data that belongs to your organization’s clients/customers/users and/or personnel without operational- justifiable reasons?

Table A.16. Results of question A.1.6 grouped by industry

	I do not know	*No*	*Yes*	**Grand Total**
Education	16.13%	41.94%	41.94%	100%
Finance/Banking	8.33%	50.00%	41.67%	100%
Public sector	36.00%	40.00%	24.00%	100%
Health	15.00%	55.00%	30.00%	100%
Others	7.69%	61.54%	30.77%	100%
Grand Total	18.81%	47.52%	33.66%	100%

Table A.17. Results of question A.1.6 grouped by gender

If you marked "yes”, have you reported that?				
	NA	No	Yes	Grand Total
Female	15.38%	53.85%	30.77%	100%
Male	60.23%	30.68%	9.09%	100%
Grand Total	54.46%	33.66%	11.88%	100%

Table A.18. Results of question A.1.6 grouped by years of experience

If you marked "yes”, have you reported that?				
	NA	No	Yes	Grand Total
2-5 years	48.15%	44.44%	7.41%	100%
Less than 2 years	61.54%	19.23%	19.23%	100%
More than five years	54.17%	35.42%	10.42%	100%
Grand Total	54.46%	33.66%	11.88%	100%

Table A.19. Results of question A.1.6 grouped by industry

If you marked "yes”, have you reported that?				
	NA	No	Yes	Grand Total
Education	51.61%	29.03%	19.35%	100%
Finance/Banking	41.67%	58.33%	0.00%	100%
Public sector	44.00%	48.00%	8.00%	100%
Health	75.00%	15.00%	10.00%	100%
Others	61.54%	23.08%	15.38%	100%
Grand Total	54.46%	33.66%	11.88%	100%

A.1.7 In your organization, are privacy-relevant operations logged and audited?

Table A.20. Results of question A.1.7 grouped by industry

	I do not know	*No*	*Yes*	**Grand Total**
Education	70.97%	9.68%	19.35%	100%
Finance/Banking	25.00%	25.00%	50.00%	100%
Public sector	52.00%	16.00%	32.00%	100%
Health	75.00%	0.00%	25.00%	100%
Others	23.08%	30.77%	46.15%	100%
Grand Total	55.45%	13.86%	30.69%	100%

A.1.8 Do you consider yourself aware of the importance of 'privacy-protection'?

Table A.21. Results of question A.1.8 grouped by gender

	No	*Yes*	**Grand Total**
Female	7.69%	92.31%	100%
Male	17.05%	82.95%	100%
Grand Total	15.84%	84.16%	100%

Table A.22 Results of question A.1.8 grouped by education level

	No	*Yes*	**Grand Total**
Bachelor	12.73%	87.27%	100%
High School	50.00%	50.00%	100%
Masters	14.29%	85.71%	100%
Ph.D.	15.79%	84.21%	100%
Grand Total	15.84%	84.16%	100%

Table A.23. Results of question A.1.8 grouped by years of experience

	No	*Yes*	**Grand Total**
2-5 years	11.11%	88.89%	100%
Less than 2 years	19.23%	80.77%	100%
More than five years	16.67%	83.33%	100%
Grand Total	15.84%	84.16%	100%

Table A.24. Results of question A.1.8 grouped by industry

	No	*Yes*	**Grand Total**
Education	19.35%	80.65%	100%
Finance/Banking	0.00%	100%	100%
Public sector	32.00%	68.00%	100%
Health	10.00%	90.00%	100%
Others	0.00%	100%	100%
Grand Total	15.84%	84.16%	100%

A.1.9 Are you aware of the IT Criminal Laws in the Kingdom of Saudi Arabia?

Table A.25. Results of question A.1.9 grouped by gender

	No	*Yes*	**Grand Total**
Female	53.85%	46.15%	100%
Male	48.86%	51.14%	100%
Grand Total	49.50%	50.50%	100%

Table A.26. Results of question A.1.9 grouped by education level

	No	*Yes*	**Grand Total**
Bachelor	49.09%	50.91%	100%
High School	50.00%	50.00%	100%
Masters	52.38%	47.62%	100%
Ph.D.	47.37%	52.63%	100%
Grand Total	49.50%	50.50%	100%

Table A.27. Results of question A.1.9 grouped by years of experience

	No	*Yes*	**Grand Total**
2-5 years	33.33%	66.67%	100%
Less than 2 years	61.54%	38.46%	100%
More than five years	52.08%	47.92%	100%
Grand Total	49.50%	50.50%	100%

Table A.28. Results of question A.1.9 grouped by industry

	No	*Yes*	**Grand Total**
Education	51.61%	48.39%	100%
Finance/Banking	33.33%	66.67%	100%
Public sector	40.00%	60.00%	100%
Health	70.00%	30.00%	100%
Others	46.15%	53.85%	100%
Grand Total	49.50%	50.50%	100%

Table 5. Results of question A.1.9 grouped by authority level

	No	*Yes*	*Grand Total*
Non decision maker	53.73%	46.27%	100%
Decision maker	41.18%	58.82%	100%
Grand Total	49.50%	50.50%	100%

A.1.10 Are you satisfied with the current status of ‘privacy-protection’ in all sectors of the Kingdom of Saudi Arabia?

Table A.29. Results of question A.1.10 grouped by gender

	No	*Yes*	**Grand Total**
Female	92.31%	7.69%	100%
Male	84.09%	15.91%	100%
Grand Total	85.15%	14.85%	100%

Table A.30. Results of question A.1.10 grouped by education level

	No	*Yes*	**Grand Total**
Bachelor	89.09%	10.91%	100%
High School	100%	0.00%	100%
Masters	80.95%	19.05%	100%
Ph.D.	73.68%	26.32%	100%
Grand Total	85.15%	14.85%	100%

Table A.31. Results of question A.1.10 grouped by years of experience

	No	*Yes*	**Grand Total**
2-5 years	92.59%	7.41%	100%
Less than 2 years	92.31%	7.69%	100%
More than five years	77.08%	22.92%	100%
Grand Total	85.15%	14.85%	100%

Table A.32. Results of question A.1.10 grouped by industry

	No	*Yes*	**Grand Total**
Education	83.87%	16.13%	100%
Finance/Banking	91.67%	8.33%	100%
Public sector	96.00%	4.00%	100%
Health	70.00%	30.00%	100%
Others	84.62%	15.38%	100%
Grand Total	85.15%	14.85%	100%

Table A.33. Results of question A.1.10 grouped by authority level

	No	*Yes*	**Grand Total**
Non decision maker	83.58%	16.42%	100%
Decision maker	88.24%	11.76%	100%
Grand Total	85.15%	14.85%	100%

A.2 Survey Questionnaires for Decision Makers

A.2.1 Is your organization adhering to any global standard of 'privacy-protection'?

Table A.34. Results of question A.2.1 grouped by industry

	I do not know	*No*	*Yes*	**Grand Total**
Education	33.33%	33.33%	33.33%	100%
Finance/Banking	25.00%	75.00%	0.00%	100%
Governmental Services	25.00%	50.00%	25.00%	100%
Health	14.29%	14.29%	71.43%	100%
Industry	33.33%	55.56%	11.11%	100%
Grand Total	26.47%	47.06%	26.47%	100%

A.2.2 Are you deploying any 'privacy-protection' system?

Table A.35. Results of question A.2.2 grouped by industry

	I do not know	*No*	*Yes*	**Grand Total**
Education	0.00%	100%	0.00%	100%
Finance/Banking	37.50%	50.00%	12.50%	100%
Governmental Services	25.00%	50.00%	25.00%	100%
Health	42.86%	28.57%	28.57%	100%
Industry	22.22%	66.67%	11.11%	100%
Grand Total	26.47%	58.82%	14.71%	100%

A.2.3 Is there a 'privacy officer' (or any similar role) in your organization?

Table A.36. Results of question A.2.3 grouped by industry

	I do not know	*No*	*Yes*	**Grand Total**
Education	0.00%	83.33%	16.67%	100%
Finance/Banking	25.00%	50.00%	25.00%	100%
Governmental Services	0.00%	100%	0.00%	100%
Health	14.29%	57.14%	28.57%	100%
Industry	11.11%	44.44%	44.44%	100%
Grand Total	11.76%	61.76%	26.47%	100%

A.2.4 How serious is your organization in protecting the privacy of its clients/customers/users and personnel?

Table A.37. Results of question A.2.4 grouped by industry

	Fairly serious	*Not serious*	*Very serious*	**Grand Total**
Education	50.00%	50.00%	0.00%	100%
Finance/Banking	25.00%	25.00%	50.00%	100%
Governmental Services	50.00%	50.00%	0.00%	100%
Health	57.14%	0.00%	42.86%	100%
Industry	55.56%	0.00%	44.44%	100%
Grand Total	47.06%	20.59%	32.35%	100%

A.2.5 Do you log and audit privacy-relevant operations?

Table A.38. Results of question A.2.5 grouped by industry

	I do not know	*No*	*Yes*	**Grand Total**
Education	33.33%	50.00%	16.67%	100%
Finance/Banking	25.00%	50.00%	25.00%	100%
Governmental Services	0.00%	75.00%	25.00%	100%
Health	28.57%	57.14%	14.29%	100%
Other	0.00%	55.56%	44.44%	100%
Grand Total	17.65%	55.88%	26.47%	100%

Table A.39. Results of question A.2.5 grouped by industry

If "yes", how frequent?							
	Always	Annually	Monthly	NA	Once a year	Quarterly	Grand Total
Education	0.00%	0.00%	0.00%	83.33%	16.67%	0.00%	100%
Finance/Banking	0.00%	0.00%	0.00%	75.00%	25.00%	0.00%	100%
Governmental Services	0.00%	0.00%	0.00%	75.00%	0.00%	25.00%	100%
Health	0.00%	0.00%	0.00%	100%	0.00%	0.00%	100%
Industry	11.11%	11.11%	11.11%	66.67%	0.00%	0.00%	100%
Grand Total	2.94%	2.94%	2.94%	79.41%	8.82%	2.94%	100%

A.2.6 Do you have a data classification policy?

Table A.40. Results of question A.2.6 grouped by industry

	I do not know	*No*	*Yes*	**Grand Total**
Education	0.00%	50.00%	50.00%	100%
Finance/Banking	25.00%	37.50%	37.50%	100%
Governmental Services	0.00%	50.00%	50.00%	100%
Health	28.57%	42.86%	28.57%	100%
Industry	22.22%	33.33%	44.44%	100%
Grand Total	17.65%	41.18%	41.18%	100%

A.2.7 Is the private data held by/at your organization encrypted?

Table A.41. Results of question A.2.7 grouped by industry

	All encrypted	*Not encrypted*	*Partially encrypted*	**Grand Total**
Education	0.00%	33.33%	66.67%	100%
Finance/Banking	25.00%	12.50%	62.50%	100%
Governmental Services	25.00%	0.00%	75.00%	100%

Health	28.57%	71.43%	0.00%	100%
Industry	11.11%	11.11%	77.78%	100%
Grand Total	17.65%	26.47%	55.88%	100%

A.2.8 Do you grant your personnel access rights to private data strictly based on a 'need-to-know' basis?

Table A.42. Results of question A.2.8 grouped by industry

	I do not know	*No*	*Yes*	**Grand Total**
Education	16.67%	50.00%	33.33%	100%
Finance/Banking	25.00%	25.00%	50.00%	100%
Governmental Services	0.00%	50.00%	50.00%	100%
Health	57.14%	14.29%	28.57%	100%
Industry	11.11%	55.56%	33.33%	100%
Grand Total	23.53%	38.24%	38.24%	100%

Table A.43. Results of question A.2.8 grouped by industry

If you marked "yes", do you audit that?				
	NA	No	Yes	Grand Total
Education	66.67%	33.33%	0.00%	100%
Finance/Banking	62.50%	25.00%	12.50%	100%
Governmental Services	50.00%	0.00%	50.00%	100%
Health	71.43%	14.29%	14.29%	100%
Industry	55.56%	22.22%	22.22%	100%
Grand Total	61.76%	20.59%	17.65%	100%

A.2.9 Is your organization subject to any national or international mandate related to personal data protection and privacy protection

Table A.44. Results of question A.2.9 grouped by industry

	I do not know	*No*	*Yes*	**Grand Total**
Education	16.67%	50.00%	33.33%	100%
Finance/Banking	37.50%	50.00%	12.50%	100%
Governmental Services	25.00%	50.00%	25.00%	100%
Health	57.14%	0.00%	42.86%	100%
Industry	44.44%	11.11%	44.44%	100%
Grand Total	38.24%	29.41%	32.35%	100%

A.2.10 Do you think that you are 'morally' obliged to preserve the privacy of your clients/customers/users and personnel?

Table A.45. Results of question A.2.10 grouped by education level

	No	*Yes*	**Grand Total**
Bachelor	25.00%	75.00%	100%
Masters	22.22%	77.78%	100%
Ph.D.	0.00%	100%	100%
Grand Total	17.65%	82.35%	100%

Table A.46. Results of question A.2.10 grouped by industry

	No	*Yes*	**Grand Total**
Education	0.00%	100%	100%
Finance/Banking	25.00%	75.00%	100%
Governmental Services	50.00%	50.00%	100%
Health	14.29%	85.71%	100%
Industry	11.11%	88.89%	100%
Grand Total	17.65%	82.35%	100%

A.2.11 Have you read the (Public Consultation Request on the Proposed Law Regulating Electronic Privacy and Data Protection in Saudi Arabia) document published by the MCIT?

Table A. 47. Results of question A.2.11 grouped by industry

	No	*Yes*	**Grand Total**
Education	66.67%	33.33%	100%
Finance/Banking	62.50%	37.50%	100%
Governmental Services	100%	0.00%	100%
Health	71.43%	28.57%	100%
Industry	88.89%	11.11%	100%
Grand Total	76.47%	23.53%	100%

Copyrights