Academic Journal of Research and Scientific Publishing | Vol 4 | Issue 39
Publication Date: 5-7-2022 ISSN: 2706-6495

The Saudi Information System Law and its Effectiveness (A Study of the Degree to Which Major Saudi Organizations Apply the Best Practices of Information Systems)

By: Amal Salama Al-Blowie

Master's in Information Systems, Shaqra University, Saudi Arabia

Amalb2040@gmail.com

Abstract:

Information Security Law is the body of legal rules, codes, and standards that require companies to protect that information and the information systems that process it from unauthorized access. The government's development, issuance, and maintenance of law requirements help to ensure that standards are met, which, in turn, supports the country's safety, productivity, and economic development. The purpose of this paper is to assess the adequacy of the current Saudi laws and regulations related to information security and the extent to which information security laws impacted companies' application of information security best practices.

The Saudi laws related to information security were studied and compared with the American information security regulations in the first part of the research. Then the experimental setting was used to perform the search by designing an electronic questionnaire to reveal the impact of Saudi information security laws on the reality of information security in companies. The questionnaire consists of 3 general questions and 11 questions regarding corporate practices that support the application of information security laws. The questionnaire was distributed to a random sample of information security workers in a number of major Saudi companies, and forty participants responded, and the largest proportion of respondents were executives, and the respondents' years of experience ranged between 1 and 40 years. It is concluded from the research that having stricter and flawless information security laws provides a strong foundation for corporate policies, and a safe investment environment.

Keywords: Information System, Saudi Law, Effectiveness, Saudi organizations, Best practices

1. Introduction

The significant development of information technology has facilitated human life and many information sources and services in real-time. However, personal and confidential information has become increasingly likely to penetrate security. Electronic intrusions and data theft can cause problems for individuals and large and significant losses for companies and institutions. In addition, they may extend to damaging the security of the national economy. Today, most companies constantly operate online. Their internal systems are used in environments that are already or easily connected to the internet, resulting in greater exposure to attack at any time. When companies are exposed to the risk of data theft and hacking, this may hurt their customers rather than the companies themselves. Occasionally, the theft of data from large companies, which directly disables their work, affects national and economic security because; information security is paramount for accurate financial reporting and timely and relevant managerial accounting reports for decision-making. (Gordon et al, 2003) An example of these attacks is the denial of service (DoS), which has lately been used to harm companies' operations and entire nations. (Czosseck et al, 2013) Some of the economic damage resulting from poor information security is associated with the costs incurred by companies in cyber-attacks. The costs associated with cyber-attacks can be divided into direct and indirect costs. Direct costs include the expenses incurred for restoring a computer system to its original, pre-attack state. Recovery from an attack will typically require extra spending on labor and materials. (Cashell, et al, 2004) Therefore, implementing information security legislation contributes to a more reliable business environment, enabling a stable economy. (Whitman & Mattord, 2010) Regulation and compliance are vital aspects of any national information technology framework regarding policy development. Therefore, protecting information and data is a shared federal responsibility for all classes in the community and reducing illegal behaviors. Government regulations must apply dissuasive and robust policies for information security. Therefore, governments should develop and update their laws and regulations, which ensure institutions' commitment to the best standards of information security and the interests of the public. This paper discusses the adequacy of the current Saudi laws and regulations related to information security and how information security laws impact companies' application of information security best practices. To achieve these goals, this paper is structured in two parts.

The first part reviews Saudi laws related to information security and compares them with the U.S. information security regulations, which stimulate companies to improve their information security.

In light of the first part's results, an electronic questionnaire was designed to determine the impact of Saudi information security laws on the reality of information security within companies.

1.2. Research objectives

The research seeks to achieve the following objectives:

- Assessing the adequacy of current Saudi laws and regulations related to information security for companies

- The impact of information security laws on the implementation of companies

- Review of Saudi laws related to information security and compare them with US information security regulations

- How information security laws in Saudi Arabia affect companies' practices

1.3. Research significance

Due to the great development in information technology, this led to the emergence of intrusion, electronic piracy and data theft, which causes problems for individuals and great losses for companies and institutions, in addition to harming the security of the national economy.

Therefore, the implementation of information security legislation contributes to economic prosperity and a more reliable business environment.

Therefore, government regulations must implement deterrent and strong information security policies and develop and update their laws and regulations related to information security. From this point of view, the importance of the research is in discussing the adequacy of the current Saudi laws and regulations related to information security and how information security laws affect companies' implementation of best information security practices

2. Laws and Regulations Related To Information Security in Saudi Arabia

In Saudi Arabia, several laws regulate certain aspects of information security. The following sections present KSA laws that apply to information security.

2.1 The Telecommunications Act (Royal Decree No. (M/12), / 03 June 2001).

According to the Saudi Telecommunications Law, intercepted information cannot be disclosed during its transmission. By the law, "it is essential to maintain strict confidentiality and privacy of telephone calls and information received or transmitted through public communication networks. Violators of such restrictions may be subject to a fine(5,000,000 Saudi Riyals) if they disclose, listen to, or record it. Further, the Telecommunications Act prohibits telecom and internet providers from disclosing information concerning their subscribers to third parties or allowing individuals access to their communications.

2.2 E-Government Implementation Rules 27/3/2006

Based on The Council of Ministers Resolution No. 40 dated 02/27/1427 H corresponding to 27/3/2006, concerning the adoption of controls to guide the implementation of e-government in government agencies, the following controls are relevant to the topic of this paper:

- Each government entity should electronically rely on information and data from relevant agencies, and the amount of information and data it needs to provide in applications and forms should be minimized.
- In most cases, no information or data will be requested from applicants unless necessary; and if it is to be used to deliver the service to the applicant.
- Each government entity must instruct its employees to comply with confidentiality and privacy protection standards.
- Information and data relevant to government service applicants shall be reviewed only by authorized personnel. In order to guarantee this right to the service user/beneficiary, the government authorities shall take all appropriate steps (Ministry of Communications and Information Technology, 2006).

2.3 The Anti-Cyber Crime Law (Royal Decree No. M/17, 1428 / 26 March 2007)

In an attempt to combat cybercrime by identifying such crimes and determining their punishment, this law has been enacted. According to KSA's Anti-Cybercrime Law, any person found guilty of:

- Accessing another's computer with the intent to delete, destroy, modify, or re-distribute its information.
- Interrupts the transmission of data through a computer or network.

The Anti-Cyber Crime law provides a good basis for prosecution of those who attack, steal, or damage networks or computers. However, it does not address prevention, education, or collaboration.

2.4 Credit Information Law (Royal Decree NO. M/37, 8 July 2008):

The purpose of this law is to establish general principles and controls for collecting, exchanging, and protecting consumer credit data (information and data on consumers regarding credit transactions, including loans, installment purchases, leases, credit sales, credit cards, and payment commitments for such transactions). Company members, government entities, and private companies that maintain credit information are subject to this law (National Center for Documents and Archives, 2008).

2.5 Penal Law on Dissemination and Disclosure of Classified Information and Documents (Royal Decree NO.M/35, 12/4/2011)

Public employees or those of the like, even after leaving their positions, should not divulge or divulge classified information or documents that they obtain or are privy to by virtue of their position, if such dissemination or disclosure remains restricted. The punishment for these acts is imprisonment for a period not exceeding twenty years or a fine not exceeding one million riyals (Penal Law on Dissemination and Disclosure of Classified Information and Documents, 2011).

After reviewing the Saudi laws, we note that Saudi laws related to information security are dispersed among several government sectors, which makes it difficult for practitioners to distribute security information cooperatively.

The laws are mainly directed at individuals and there is rarely a law, which requires companies to apply national or international standards to ensure information security.

3. U.S. Information security laws

The U.S. is one of the leading countries that regulate information security issues. Next, we will examine several U.S. laws that have a significant impact on businesses when they implement best practices of information security. To my knowledge, these laws do not exist concerning Saudi Arabian information security.

3.1 Security breach notification statutes

These are laws requiring an organization that loses control of an individual's "personal information" to disclose that loss to those concerned. As of October 2010, 46 states, including the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, have such laws. These laws were originally designed to protect consumers against identity theft by requiring data custodians to notify individuals when they lost control of information that could facilitate identity theft (Thaw, 2011).

3.2 The Gramm-Leach-Bliley Financial Modernization Act of 1999 ("GLBA")

Specifies requirements for the safeguarding of financial institutions. These safeguards require that: To ensure that the financial institutions within the jurisdiction of each agency or authority are adequately protected in administrative, technical, and physical ways, each agency or authority shall establish appropriate standards. (1) To keep customer information secure and confidential; (2) To guard against any threats or hazards which would threaten the security or integrity of such information; and (3) To protect against unauthorized access to or use of such information or records that might cause considerable harm or inconvenience to customers (Thaw, 2011).

3.3 Gramm-Leach-Bliley Financial Modernization Act ("GLBA")

Gramm-Leach-Bliley Act requires financial institutions, which offer products and services to consumers, such as loans, financial advice or insurance, to explain their information-sharing policies to their customers and to protect sensitive information (Federal Trade Commission, 1999).

3.4 Massachusetts Standards for the Protection of Personal Information of Commonwealth

Residents this regulation establishes minimum standards that must be met to ensure that both paper and electronic records that contain personal information are protected. These regulations are intended to ensure that consumer information is secure and confidential in a manner in keeping with industry standards and to safeguard against anticipated threats to the integrity, security, and security of such information, as well as protect against unauthorized access to or use of that information which may result in considerable harm or inconvenience for consumers.

The law states that personal information must be encrypted when stored on portable devices or transmitted wirelessly or on public networks. According to additional requirements, businesses need to employ up-to-date firewall protection to safeguard their data from the outside world and limit access to or transmission of data to authorized users only, in accordance with established policies. (Thaw, 2011) In addition, the act contains the duty to Protect and Standards for Protecting Personal Information and Computer System Security Requirements (The Official Website of the Attorney General of Massachusetts, 2010).

4. Methodology

This section describes in detail the experimental setup used to conduct the research within this work.

How Do The KSA Information Security Laws Affect Companies' Application To Information Security Best Practices?

After reviewing the laws that support information security in Saudi Arabia, an electronic questionnaire was built to detect the impact of the Saudi information security laws on the reality of information security in companies. The questionnaire was composed of 3 general questions and 11 questions regarding the practices of companies that support the application of the laws on information security. The questionnaire was distributed to a random sample of employees involved in information security at several major Saudi companies. Seventy-five questionnaires were sent via email and Twitter to those responsible for information security in several major Saudi companies within a variety of vital sectors. Forty participants responded from the following sectors:

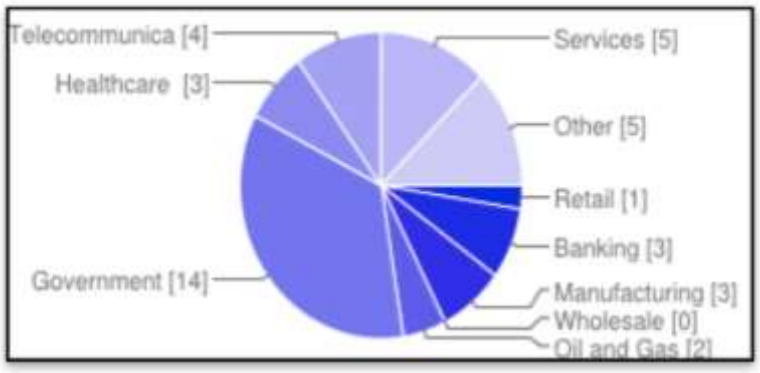


Figure (1): distribution of respondents by sector

The largest proportion of respondents were executive managers. The following chart shows the distribution in terms of the jobs held by participants. The years of respondents' experience ranged between 1 and 40 years.

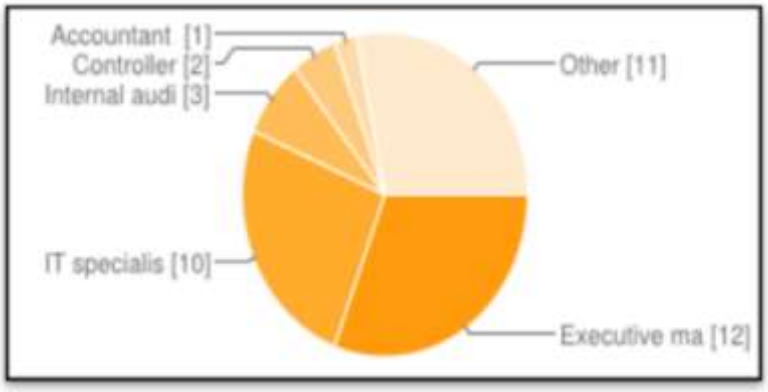
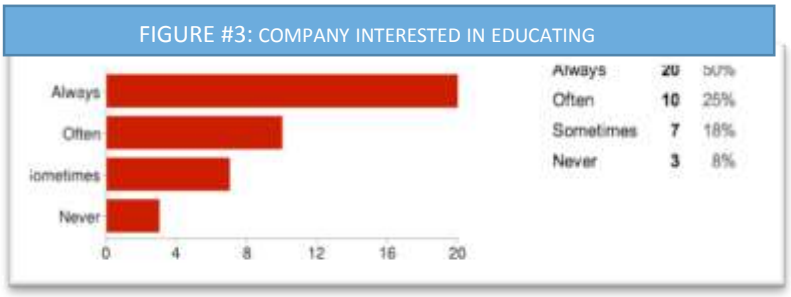


Figure. (2): Distribution of respondents' jobs.

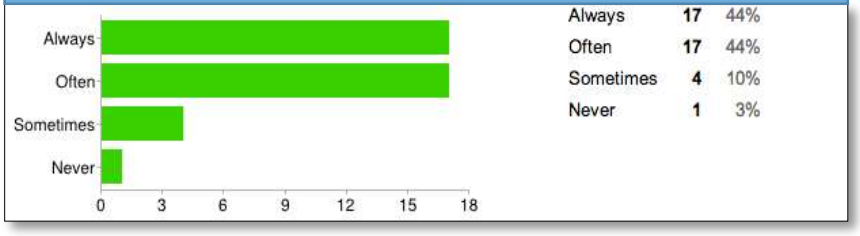
5. Results and Discussion

1- Do the information security practitioners within your organization endeavor to understand the current Saudi IS legal environment?



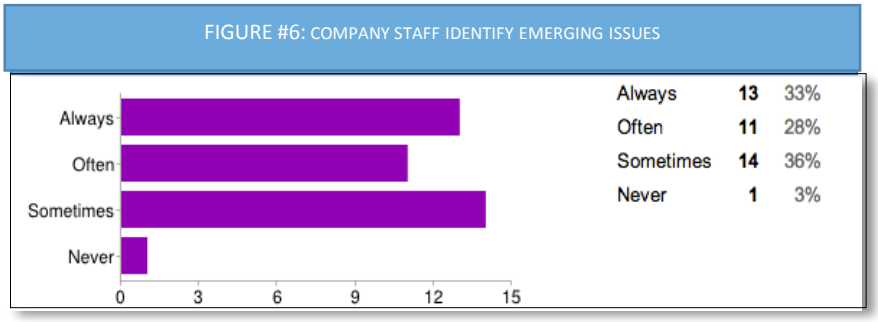
2- Do the information security practitioners within your organization endeavor to stay current with regards to Saudi IS laws and regulations?

FIGURE #5: STAFF STAY CURRENT WITH SAUDI IS



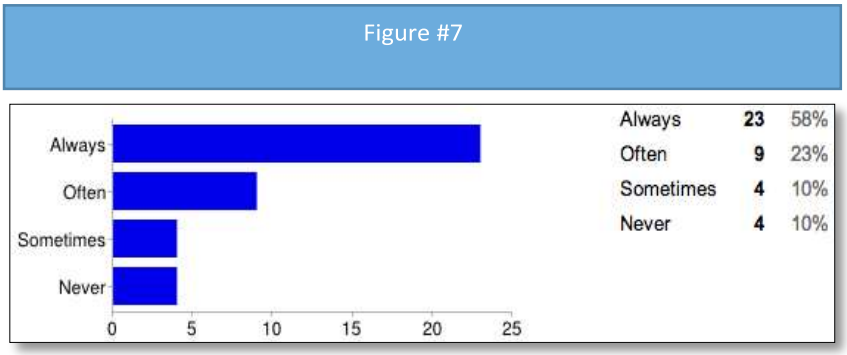
3- Do the security practitioners in your organization endeavour to identify emerging issues?

FIGURE #6: COMPANY STAFF IDENTIFY EMERGING ISSUES



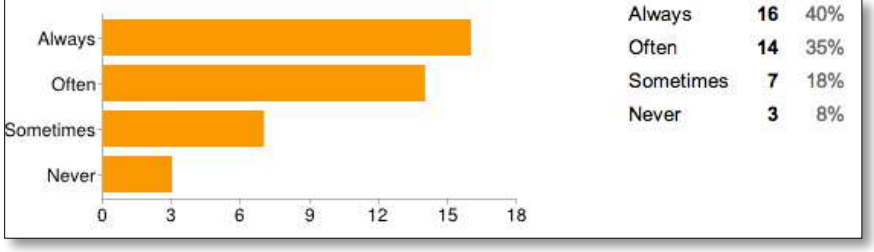
4- Does the security policy in your companysupport the Saudi information security laws?

Figure #7



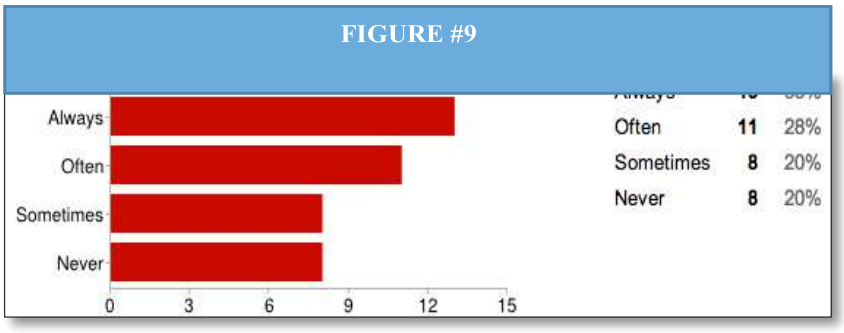
5- Do information security officials in your company endeavour to educate employees about laws which carry sanctions and the responsibilityof both the company and the employee? (i.e. distributing awareness leaflets, awareness emailsand awareness lectures).

FIGURE #8: COMPANY INTERESTED IN EDUCATING STAFF



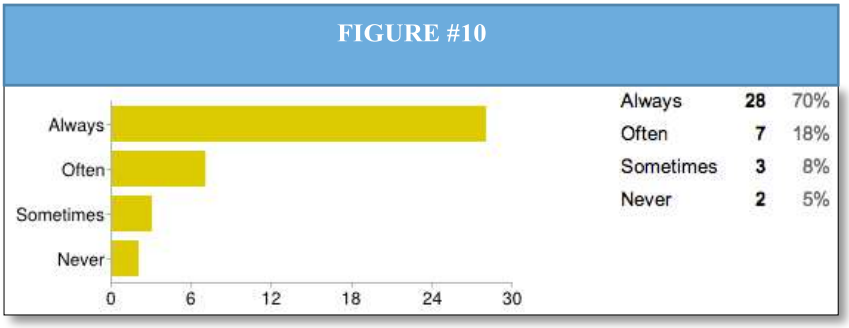
6- Are the information security officials within the company insuring that employees know what constitutes acceptable behavior; and do they know about the consequences of illegal or unethical actions.

FIGURE #9



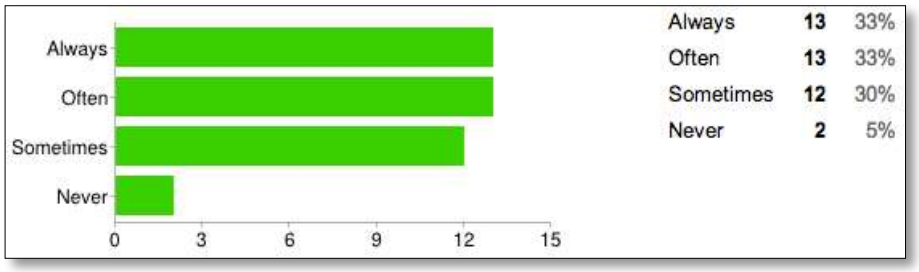
7- Does the company use technology to control employee access to information as necessary (suchas a firewall) to protect confidential and personal data from criminal action?

FIGURE #10



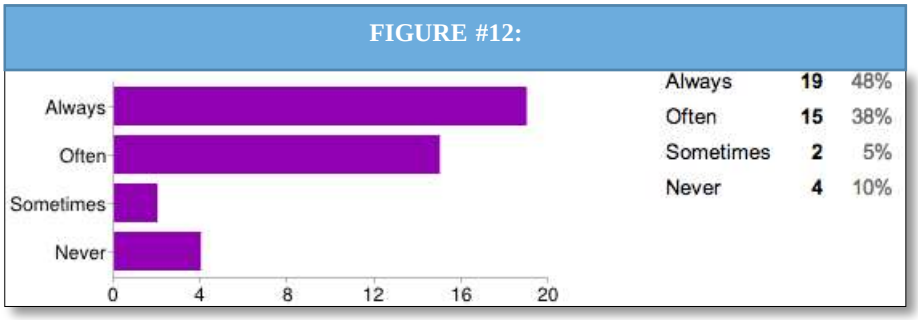
8- Does the company makes a valid effort to protectothers and continually maintain that effort?

FIGURE #11



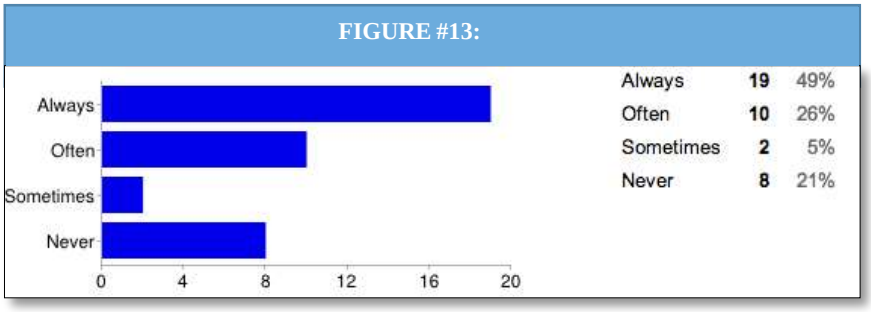
9- Does the company monitor the commitment ofemployees in the information security laws?

FIGURE #12:



10- Does the company implement strict penalties against employees who break laws? (i.e. publishingconfidential information, listening or recording data intercepted during transmission?

FIGURE #13:



5.1. Key Findings From the Survey Include the Following:

• Educating employees about the laws of information security and privacy protection are important issues. This is because people are one of the greatest threats to information security and are the weakest link in a security chain.

Policy, education and training, awareness, and technology should be employed appropriately to

prevent people from accidentally or intentionally damaging or losing information. (Whitman & Mattord, 2010) Therefore laws are gaining importance by applying their people and commitment to them. Thus awareness about the laws and their application through companies' security policies is a key role for the Department of Information Security within companies (Guide for the Roles and Responsibilities of an Information Security Officer Within State Government, 2008). The survey results showed that the majority of respondents confirmed that their companies were interested in educating and sensitizing their employees to information security laws. This result was evident through the participants' answers to Question 1, where half of the sample responded that the company was always interested in educating its employees. One-third of the sample often answered (see Figure. 2).

The answers to the sixth Question confirmed that the company officials made an effort to educate their employees, with 80% of the sample providing an answer of always and often (see Figure. 8).

• Usually, all individuals and institutions endeavor to follow the law and avoid breaching the laws for fear of punishment and therefore take responsibility. This is evident from the respondents' responses to Questions 2, 3, and 4, which confirm that 80% of the respondents were keen to understand the legal environment within Saudi Arabia (see Figure. 4) In answer to Question. 3 90% followed the updates regarding the laws of information security (see Figure. 5). In addition, 60% were keen to follow up on legal issues (Figure. 6).

• Whatever the efforts of legislators to develop laws and policies, these laws are deterrents only if the availability of the three conditions: Fear of penalty, probability of being caught, and probability of a penalty, are being administered. (Whitman & Mattord, 2010) Therefore, monitoring the performance of employees and the application of sanctions against violators is an integral part of law enforcement. Participants' responses in the survey reflected there to be a problem in the control and the application of sanctions against violators, as seen from the answers to Question number 7, whereby 40% of officials were unsure whether their employees applied the laws. Answers to Question 11 indicated that 25% of respondents believed that employees were safe from punishment in the event of penetration by the law. This should be treated seriously because it reduces the importance of the laws and their role in maintaining security.

• In Question 5, 90% of the participants stressed that the company's policy supported the laws of Saudi Arabia, and this is to be expected because local laws are one of the sources of security

policy for companies. Therefore, government regulations play a role in corporate practices and their employees. Whereas the prospect of being sued for damages when confidential information is stolen or destroyed is a major incentive for companies to improve their information security. Lower liability would also reduce the incentive to invest in security. (Cashell, et al, 2004).

• Observed from the foregoing that the companies claim that they applied the laws of information security in Saudi Arabia is shown by the responses of respondents. However, we find that the level of information security in Saudi Arabia is low. This is what Drashalgthber and Sabeeh confirmed; the study reported that the level of information security in Saudi Arabia is less than required (Alghathbar, 2012).

This may be due to the weakness of the legal structure related to information security that does not require companies to apply standards and the minimum requirements for information security.

6. Suggestions

A number of suggestions, which may have a positive impact for improving the environment for information security, have been provided:

- The speed of development and the application of the document to the National Information Security.

- Motivating companies to apply the best practices of information security through rewards Certified Companies applying information security standards.

- Building a national database to share information about best practices for information security and the potential dangers and the experiences of companies in responding to electronic attacks.

7. Conclusion

It has been demonstrated that the laws of information security provide a strong foundation for company policies. These are derived from security laws, and the IS laws reflect the practices of security companies, for either the better or worse, because where a greater stringent legal environmentfree of gaps exists, the practices of security companies will be improved. This in turn provides a safe environment for investment.

8. References

Gordon L.A., Loeb M.P., and Lucyshyn W., (2003) *Sharing information on computer systems security: An economic analysis.* Journal of Accounting and Public Policy. **22**(6): p. 461-485.

Czosseck C., Ottis R., and Taliharm A.-M. (2013). *Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security.* Case Studies in Information Warfare and Security: For Researchers, Teachers and Students. p. 72.

Cashell, B., et al. (2004). *The economic impact of cyber-attacks*. Congressional Research Service, Library of Congress.

Whitman, M.E. and Mattord H.J. (2010). *Principles of information security*. Cengage Learning.

Communications and Information Technology Commission (2007). Anti-Cyber Crime Law

Communications and Information TechnologyCommission. (2007). The Electronic Transactions Law

Communications and Information Technology Commission (2001). The Telecommunications Act.

Penal Law on Dissemination and Disclosure of Classified Information and Documents (2011).

National Center for Documents and Archives. (2008). Credit Information Law.

Ministry of Communications and Information Technology. (2006). E-Government Implementation Rules.

Thaw, D.B., (2011). Characterizing, Classifying, and Understanding Information Security Laws and Regulations: Considerations for Policymakers and Organizations Protecting Sensitive Information Assets. ERIC.

Federal Trade Commission. (1999). Financial Privacy: The Gramm–Leach–Bliley Act.

The Official Website of the Attorney General of Massachusetts (2010). 201 CMR 17.00: STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH.

Guide for the Roles and Responsibilities of an Information Security Officer within State Government (2008). O.o.I.S.a.P. Protection.

Alghathbar, S., (2012). *Case of information security in Saudi Arabia.* Information Studies. 14

Doi: doi.org/10.52132/Ajrsp.e.2022.39.2