Pertanika J. Sci. & Technol. 30 (3): 1909 - 1926 (2022)

PERTANIKA JOURNALS

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

Vulnerability of Saudi Private Sector Organisations to Cyber Threats and Methods to Reduce the Vulnerability

Emad Shafie

Department of Computer and Applied Science, Applied College, Umm Al-Qura University, 715 Saudi Arabia

ABSTRACT

The Middle Eastern region has witnessed many cyber-attacks in recent years, especially in Saudi Arabia. Saudi Arabian organisations face problems anticipating, detecting, mitigating, or preventing cyber-attacks despite policies and regulations. The reasons for this have not been investigated adequately. This research aims to study the methods used to address cyber security issues in the private sector. A survey of IT managers of private organisations yielded 230 usable responses. The data were analysed for descriptive statistics and frequency estimations of responses, and the results are presented in this paper. Poor awareness of cyber security issues is reflected in the survey responses. The expenditure on cyber security, especially by large firms, was inadequate. There was a greater tendency to outsource many aspects of cyber security without concern about the risks. A very small percentage of IT managers considered the certainty of a cyber threat within the next year. It is important from the point of proactive strategies to prevent attacks. The findings highlight a lack of required knowledge and skills in performing their expected roles well. Additionally, many weaknesses have been detected in cyber security management in Saudi private organisations, and there is room to improve the quality of computer security systems. The published literature largely supported this. The findings from this study have implications for the stakeholders, especially IT managers working in the private sector of Saudi Arabia. The learnings from this study may be used to address the vulnerabilities identified. The findings clearly show the need to train IT managers of Saudi private organisations.

Keywords: Awareness survey, computer security, database systems, quality improvement, Saudi Arabia

ARTICLE INFO

Article history:
Received: 6 November 2021
Accepted: 7 February 2022
Published: 20 April 2022

DOI: https://doi.org/10.47836/pjst.30.3.08

E-mail address:
eashafie@uqu.edu.sa (Emad Shafie)

ISSN: 0128-7680
e-ISSN: 2231-8526

INTRODUCTION

The occurrence of cybercrimes has increased in recent years. In 2020, Interpol reported that the global health crisis due to Covid-19 had been further complicated by cyber-attacks related to the pandemic, thereby causing a considerable strain on healthcare and law enforcement authorities worldwide. It is estimated that approximately 907,000 spam messages, 737 incidents related to the malware, and 48,000 malicious URLs, all related to Covid-19, were identified between January and April 2020. The attacks have increasingly been aimed at big corporations, governments, and critical infrastructure, all of which have a significant role in dealing with the pandemic. Out of 194 countries, 48 participated in an Interpol survey from April to May 2020. Thirteen private partners provided additional data. The results showed Europe sharing 42% of the attacks and the MENA region sharing 10% of the attacks. The types of attacks were online phishing and scams (most frequent), disruptive malware such as DDoS, data harvesting malware, malicious domains, and misinformation (Stock, 2020).

The global costs of cybercrime increased from $3 trillion in 2015 to $6 trillion in 2021 and are expected to increase further to over $10.5 trillion by 2025. These estimates do not include non-monetary cybercrimes like violence, stalking, and sexual exploitation through the internet (Hawdon, 2021).

Most cyber-attacks occur due to a lack of awareness and vigil when dealing with the internet leading to inadvertent actions which attract cyber-attackers. Therefore, the main issue arising from the above trends is creating awareness to reduce vulnerability to cyberattacks at all levels.

Saudi Arabia continues to be a key target for cyberattacks due to its oil resources and its location in the geopolitically tense Middle East. The International Data Corporation's (IDC) most recent Chief Information Officer (CIO) Survey conducted in Saudi Arabia revealed that about 60% of Saudi CIOs perceive their biggest technological challenge as cyber security management. The impact of this perception may be on about 46% of Saudi CIOs. An estimated 75% of them have their highest priority business objective as investments in privacy and cybersecurity, especially with their digital transformation agendas. Cyber security readiness is becoming an important performance indicator of Saudi Arabian firms for addressing the country's goals for achieving its Vision 2030 (Wright & Allan, 2020). These observations show that lack of awareness by internet users leads to increased vulnerability to cyber-attacks. The global observation of creating increased awareness to reduce vulnerability is equally important to Saudi Arabia.

Hence, this research investigates the awareness and the methods used to address cyber security issues in the Saudi private sector. It is the opportune moment for such a study because Saudi Arabia, as in the case of the rest of the world, is during the new waves of delta and Omicron variants of the covid pandemic, providing cybercriminals with an excellent opportunity for their nefarious activities. The intention is to use the survey findings to recommend improvements in the current database systems of Saudi private sectors for enhanced cyber security.

The findings show that IT managers of Saudi private organisations are not adequately aware of the issues related to cyber security and how to protect and mitigate cyber security breaches. These observations stress the need to train them on possible types of cyber security breaches, proactive and mitigation strategies.

The rest of this paper is organised in the following manner. The next section reviews the published literature related to the topic to justify this study. It is followed by the Methodology section describing the procedure adopted for collecting and analysing data to achieve the aim of this study. The results obtained from the collected and analysed data are presented in the Results section. These results are discussed, interpreted and explained with the literature support in the Discussion section. The Conclusion section captures the main points of this research. Some recommendations to improve cyber security in Saudi private organisations are derived from the findings listed in the Recommendations section. Finally, some limitations of the study are enumerated with explanations.

LITERATURE REVIEW

The vulnerability to cyber-attacks increases with the increasing use of the internet. The rapid increase in internet and social media use by Saudi people makes them increasingly vulnerable. According to the statistics published by ITU (2021), 4.9 billion people (63% of the population) were using the internet in 2021 worldwide. About 66% of the Arab population was using the internet this year. More male and young population in urban areas was using the internet than the female and older population in rural areas. The Middle East and specifically Saudi Arabia, have witnessed a surge in the number of internet users, reaching approximately 22.4 million in 2016 (Alzarhani & Alomar, 2016) and 33.58 million out of an estimated population of 35.08 million (95% of the population are internet users) in 2021, spending an average of 7 hrs and 45 minutes on the internet (The Global Statistics, 2022). There is also a substantial increase in different internet services in Saudi Arabia. According to GMI (2021), 27.8 million (79.25% of the population) use and spend about three hours daily on social media. More than 25 million (70%) of the population uses YouTube, Instagram, Facebook, and Twitter. Most people send and receive messages on WhatsApp (80%), followed by Facebook and Snapchat (about 54%). Men and the younger generation see social media ads more than women and the older generation. It has meant that the number of internet users has increased over the years, and the variety of services utilising the internet and providing their services online has also risen. The Saudi population's increased vulnerability due to increased internet and online services usage is compounded by a lack of Information Security Awareness (ISA) found in Saudi Arabia (Alzarhani & Alomar, 2016).

Cybercrimes include a host of different activities such as hacking, identity theft, virus dissemination, denial of service attack, phishing, spamming, cyberstalking, and cyber terrorism, to name a few (Elnaim, 2013). In Saudi Arabia, the largest cyber-attack took place on the Aramco oil plant in August 2012. A Shamoon virus attack damaged an estimated 30,000 computers to stop oil and gas production at the biggest OPEC exporter. Aramco had been the prime target for repeated cyber-attacks with malware like Emotet. Increased frequency of attacks was noted even as late as the final quarter of 2019 (Hydrocarbon Processing, 2020). However, Aramco had been able to survive these attacks through methodical strategies. Many other companies in Saudi Arabia may not have had the resources and know-how to do so. The Aramco incidences show how awareness helps to devise strategies against cyber-attacks.

According to Perlroth and Krauss (2018), the August 2012 attack was meant to trigger an explosion. Instead, it represented the threatening intensification of international hacking by anonymous operatives who possessed the drive and the ability to cause severe physical damage. The incident also posed a similar threat to other countries.

In 2017 there was a string of hacking attacks on petrochemical plants in Saudi Arabia. Computer screens went blank at the National Industrialization Company (Tasnee), one of the very few privately owned Saudi petrochemical companies leading to the hard drives being destroyed and data erased to appear the image of a Syrian child who had drowned off the Turkey coast when the family was fleeing civil war. Thus, a political message was also intended. Simultaneously, about 15 miles away, computers crashed at Sadara Chemical Company, a joint venture between Saudi Aramco and Dow Chemical. These attacks thwart Crown Prince Mohammed bin Salman's aim to accelerate Saudi Arabia's economic growth through private participation and diversification from oil. The attack on a private oil processing firm was interpreted as an indication. This attack compromised the computerised controllers, which are also used for many worldwide applications. The official website of King Saud University, too, suffered a hack by unknown entities, which led to a data dump of users' information (Alzarhani & Alomar, 2016). Therefore, these attacks exposed the vulnerability of even the most dependable systems in the country. The success of cyber-attacks on private firms shows how the lack of awareness can prevent implementing strategies to protect vital installations.

It is even more alarming when the study by Kaspersky Lab states that approximately 60% of institutions in Saudi Arabia have experienced virus and malware attacks from August 2016 to August 2017 (Alshammari & Singh, 2018). Another alarming statistic is that from 2012, 40% of social media users in the country fell victim to some cybercrime. In the same year, such cybercrimes cost the country approximately $693 million (Alshammari & Singh, 2018). Therefore, it is evident that cybercrime is on the rise in Saudi Arabia and requires strict and effective measures to prevent them from reducing the cost burden.

In the wider context of the region, poor preparedness against cyber-attacks in Muslim countries could be the cause of recent increased incidences of grave impacts in Saudi Arabia and a few other Muslim countries (Basamh et al., 2014). The need for organisational efforts to enhance the awareness and skills to deal with cyber threats was highlighted by AlMindeel and Martins (2020) through a single case study of a Saudi public organisation. The required knowledge involves an awareness of information security, knowledge, and behaviour at individual levels. Customisation to the needs of stakeholders, the organisational needs, integration of both electronic and physical learning resources, and a range of other factors all facilitate this.

Cyber Security Awareness in Saudi Arabia

Some recent findings on the cyber security awareness of Saudi people are reviewed here. Earlier works have been cited and discussed already in the discussed works (Alotaibi et al., 2016; Alsmadi & Zarour, 2018; Alotaibi, 2019; AlMindeel & Martins, 2020; Alzubaidi, 2021).

Very limited awareness was noted among Saudi people about cyber security and the role of the government and other organisations in ensuring cyber safety, despite their good knowledge about IT, from an online survey by Alotaibi et al. (2016). A low level of awareness leading to high-risk internet behaviour among Saudi people was also reported by Alzubaidi (2021), with the second-highest cyber security breachers attracting cyber-attacks due to its wealth and high level of active internet and social media uses. Many researchers observed this lack of awareness among regions, industry sectors, types of internet services, attacks, and specific demographic groups. A low level of cyber security awareness and a preference for mobile applications for learning about cyber security was observed among a sample of the Saudi population in a survey by Alotaibi (2019). The need for information security awareness among employees was highlighted using a case study of a government organisation by AlMindeel and Martins (2020). Alsmadi and Zarour's (2018) survey results showed that many Saudi Arabian people knew security tools, but many did not know or use them. Employers had provided no awareness or training programmes on cyber security or mitigating methods. As a result, most Saudis did not know how to or did not report cybercrimes. Healthcare, financial, technology, multiple, individual/private, and public sectors were particularly vulnerable to cyber-attacks; hence, these sectors need to be given priority for awareness training programmes.

Saudi Government Initiatives to Solve the Problems

The government has taken several initiatives to address the growing risk of cyber-attacks in Saudi Arabia. The Communications and Information Technology Commission (CITC) initiative was set up in 2005. It is equipped with the responsibility of regulating 'the necessary organisational procedures and implementing policies and laws enacted by the government in the sphere of IT' (Quadri & Khan, 2019). In addition, the Commission grants licenses and upholds Saudi statutes about IT and cybersecurity. This Commission also has the power to identify and block websites that it mandates as being inappropriate or dangerous.

Another step the government took in tackling cybersecurity was the setting up the Computer Emergency Response Team (CERT) in 2006. This team works under the CITC to spread awareness about cybersecurity threats in the country and how to mitigate them.

In 2007, Saudi Arabia issued a cybercrime law known as the Anti-Cyber Crime Law or ACCL. The law aims to protect information security and protect against identity theft, piracy, and other cybercrimes (Alshammari & Singh, 2018).

In addition to this, the National Cybersecurity Authority (NCA) was established in 2017 with the aim 'to boost the state cybersecurity and defend the national infrastructure' (Quadri & Khan, 2019). The NCA is mandated to achieve this goal by analysing, drafting, mandating, and regulating 'cybersecurity policies, frameworks, criteria, and guidelines' (Quadri & Khan, 2019). Furthermore, as per Saudi Vision 2030, the NCA must create 'a national cybersecurity industry' to enable Saudi Arabia to become a 'leader in cybersecurity in the region' (Quadri & Khan, 2019). Hence, it is evident that the government has taken steps in the right direction to address the threats posed by the spate of cyber-attacks and further enhance its cybersecurity infrastructure.

It must be mentioned here that although the relevant laws exist in Saudi Arabia to address cybersecurity, there is a corresponding need to raise awareness among citizens regarding safe usage of the internet. Spreading awareness about the financial impact of cybercrimes may be a step in the right direction.

The literature review reveals, therefore, the vulnerability of Saudi Arabia's cybersecurity infrastructure. The government has enacted certain laws and made provisions that treat cybercrimes as punishable offences to address this vulnerability. While this is a step in the right direction, simultaneous efforts must also be made to spread awareness about cyberattacks' nature, types, and impact. It is essential to ensure that people remain vigilant and avoid falling into traps laid out by criminals online. It is even more relevant in Covid-19, which has seen an escalation in online services, especially for education, shopping, financial services, and health. Many people access goods and services online and may be vulnerable to cyberattacks. While effective laws must be in place to punish those who perpetrate such crimes, they must go hand in hand with raising awareness levels.

Based on the observation that the Saudi people preferred mobile applications for cyber security tools, Alotaibi (2019) developed two mobile-based game applications to enhance cyber security awareness. In a detailed discussion, Alshammari and Singh (2018) observed that to solve the cyber security issues, Saudi Arabia enacted the anti-cybercrimes law in

2007. Anti-cybercrimes law covers important areas to fight against cybercrimes and states their penalties. However, it is deficient in protecting against identity theft and invasion of privacy. As a result, the country is among the top ranks in cyber security measures. The Global Cyber-Security Index of 2017 placed Saudi Arabia in the maturing stage behind the leading nations. Thus, Saudi Arabia may be considered a semi-prepared nation concerning the capability to defend itself against cybercrimes. To improve its GCI ranking to the top levels, Saudi Arabia needs to strengthen its cybercrimes law, cyber-security regulations and authorities. Also, it is important to develop clear cyber-security strategies, standards, metrics, and R&D programs. Furthermore, the domestic cyber-security industry needs to be promoted by incentivising them and encouraging them into multi-lateral agreements.

Talib et al. (2018) proposed an ontology-based cyber security policy for Saudi Arabia. The ontological approach aims to arrive at a desirable cyber security strategic environment by identifying and suggesting a formal, encoded description. A multi-layered protection strategy specifying their roles, responsibilities, and obligations was the core of the strategic environment.

Three models, derived from the basic model of NIST, for the cyber security of Saudi SMEs in the education, healthcare, and commercial sectors were developed by Ajmi et al. (2019). These models help to identify cyber threats of different types based on the structure of the SMEs.

METHODOLOGY

This study uses quantitative methods, relying on data collection and analysis. Quantitative methods may be understood as scientific and precise, relying on statistical analysis to draw inferences. These inferences may then inform the results drawn. It may be said that quantitative methods emphasise measurable data. Quantitative research can best be understood as being data-oriented. Adopting such methods has several advantages. It is possible to arrive at a definitive and precise answer to the research question through quantitative research. The results may be generalised to a larger target group depending on the sample. However, these methods also have their disadvantages. While it is possible to arrive at a clear solution through quantitative methods, they do not provide the 'why' or 'how' behind the data collected.

Quantitative methods are different from qualitative methods. Qualitative research seeks to understand the 'how' and 'why' behind the phenomenon and data; those are less tangible and difficult to quantify. Studies may choose to adopt qualitative, quantitative, or mixed methods.

For this study, it was determined that choosing quantitative methods would be useful.

Several tools may be adopted while conducting a quantitative study. Examples of such tools include surveys, interviews, and questionnaires. Once the sample is determined for the study, data is collected. This data is then analysed using statistical tools through which the results may be interpreted.

A study conducted a computer security awareness survey on Saudi private sector firms. A simple questionnaire was designed to capture the basic characteristics of the company and the computer security awareness of its employees. The questionnaires were adapted from the literature to the Saudi context. The objective was to understand the extent and factors affecting cyber security awareness among the Saudi public, which can facilitate the recommendation of protection strategies.

The IT managers of the companies participated in the survey. The participants were contacted via email, and their contact information was obtained from private sector business directories (e.g., https://www.eyeofriyadh.com/directory) in Saudi Arabia. The survey was deployed in Survey Monkey and contained a cover letter describing the purpose of the research and the voluntary nature of participation. The cover letter also advised the potential participants that they were free to withdraw at any point, and their private details were not being collected. The link to the survey questionnaire in Survey Monkey was emailed to more than 1000 people, from which 230 usable responses were obtained, giving an overall response rate of 23%. The results of this survey are presented in the following section.

All ethical requirements of conducting research using human beings have complied with university regulations. The required permissions were obtained. The privacy and confidentiality of participants were ensured. The hard copies and electronic data of the research were fully protected from theft, malware attacks on the laptop, and other likely losses.

RESULTS

Industry Profile of Survey Participants

The profile of industries sampled for this survey is given below in Table 1. It depicts that more than half (53%) of the participants were from the construction sector. Manufacturing (approximately 15%) and retail (about 8%) were the next two sectors of highest participation. All the others were <5%.

Table 1

Sample distribution by industry

Industry	Number of participants	Percentage
Construction	122	53.0%
Manufacturing	34	14.8%

Table 1 *(Continue)*

Industry	Number of participants	Percentage
Electricity, Gas, Water and Waste Services	7	3.0%
Mining, Oil and Gas	11	4.8%
Retail Trade	19	8.3%
Accommodation and Food Services	6	2.6%
Transport, Postal and Warehousing	9	3.9%
Information Media and Telecommunications	3	1.3%
Financial and Insurance Services	5	2.2%
Administrative and Support Services	5	2.2%
Public Administration and Safety	2	0.9%
Education and Training	3	1.3%
Health Care and Social Assistance	4	1.7%
Total	230	100.0%

Cyber Security Expenditure

The seriousness attached to the issue of cyber security will be evident from the amount spent by any company to ensure the security and privacy of their data and transactions. Figure 1 provides the amounts spent by the sampled companies on cyber security every year.

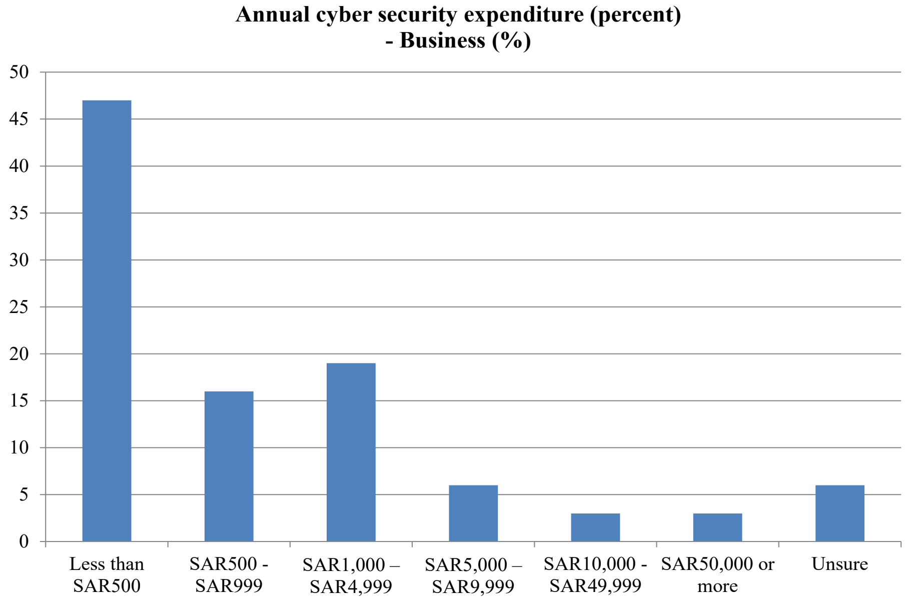

Figure 1. Annual cyber security expenditure of Saudi private organisations

About 82% of the firms spent less than SAR 5000/ per annum. Nearly half (47%) spent a nominal SAR 500 or less on this. Only 6% of the companies spent SAR 10000 or more. The amounts spent may reflect their unawareness of the seriousness of cyber security, no record of such instances, or just the risk-taking behaviour of the management.

Gross Income of the Participating Firms

Relative cyber security threats and the need to spend on cyber security may be related to the company's gross income. Cyber attackers may not be interested in the small stakes of low-income firms. However, the threat may be real in the case of high-income firms. However, no cut-off income can be placed on the probability of cyber threats. Figure 2 below provides the frequency of firms in different gross income ranges.

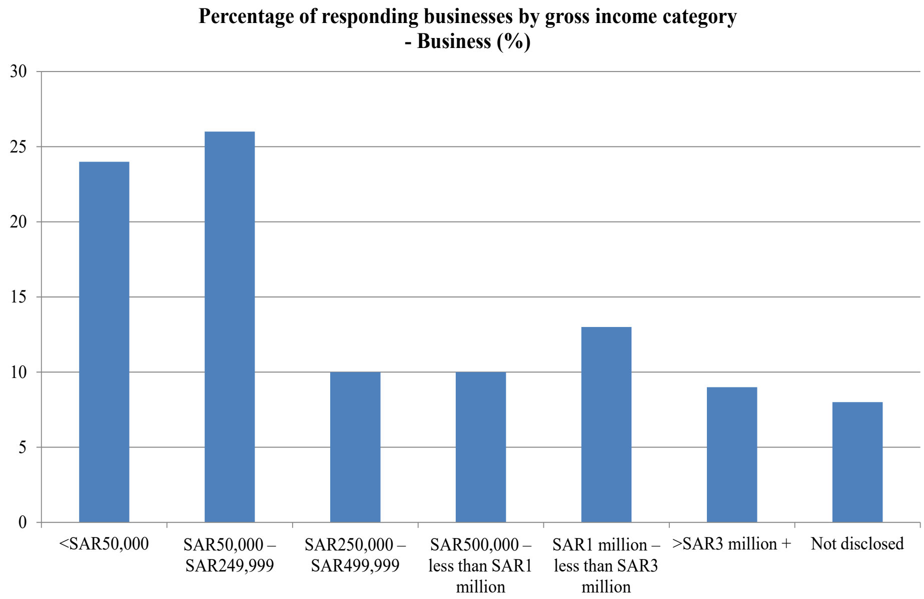

Figure 2. Percentage of businesses based on their gross income ranges

According to data in Figure 2, the gross income of approximately 70% of the firms is less than a million SAR. Cyber attackers may not be interested in these firms. However, cyber threat is a strong possibility for the remaining 30 firms with higher than 1 million SAR. In this respect, the study assumes that the 8% not disclosed belongs to the high-income group, so they do not want to disclose. Sizeable expenditure on cyber security (10000 or more SAR) in Table 2 was seen only by 12% of the firms sampled. Suppose this 12% represents the high-income firms (as low-income firms cannot afford it), leaving about 18% of high-income firms doing nothing to protect their data and transactions. The stakeholders with whom they are in contact may also be vulnerable due to this reason.

IT Security Outsourcing

A firm may outsource security as a management strategy or out of compulsion like lack of resources or expertise or being too small to have a separate system. In Table 2, the scenario related to outsourcing based on the size of the business in terms of employee size is presented.

Table 2

Responsibility for IT security management by business size (per cent)

Business size	Internal and outsourced IT response (per cent)	
	Internal IT security	Outsourced sourced IT security
1 person company	98	2
2–4 employees	90	10
5–19 employees	60	40
20–199 employees	55	45

The general trend in Table 2 is the tendency of bigger firms to outsource their cybersecurity responsibility. The threat is real and big for them, and they may like experts to handle this issue. Smaller firms may not have to face cyber threats due to their unattractiveness. Single-person companies may not be too concerned about it or may not be aware of these issues. Hence, the requirement and outsourcing of cyber security are very low in their cases.

Security Aspects Outsourced

Within outsourcing, not all aspects are outsourced as a complete package in most cases. The company may prefer to handle smaller problems by themselves. For example, where outsourcing involves compromising business secrets or sensitive data, such aspects may not be outsourced. Thus, many times, only certain aspects of cyber security may be selectively outsourced due to a lack of expertise or resources. This picture is clear from the data presented in Figure 3.

Restricted admin access, disabling macros, and daily backups could be handled by them, as they do not involve the use of complicated protection systems. However, allowlisting, patching applications, system operations, and hardening applications require sufficient expertise even for daily management. So, these were best outsourced.

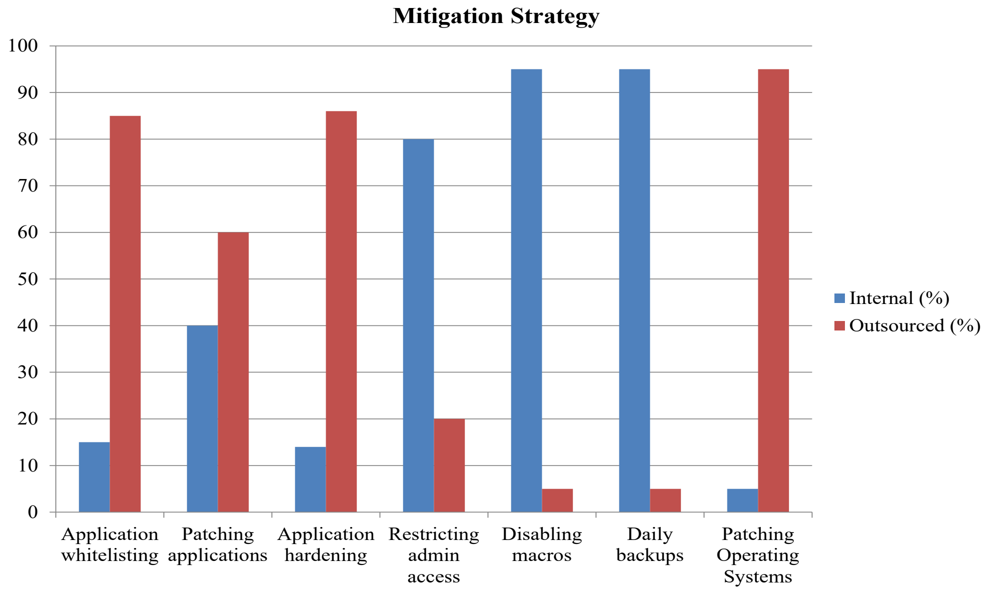

Figure 3. IT security aspects outsourced

Risk Assessment

One of the duties of IT managers is to assess and manage the cyber security risks of the company. Table 3 provides the data on how these managers did this in their firms.

Table 3

Self-assessed risk of experiencing a cyber incident in the next year

	Risk of experiencing a cyber incident	
Category	n	%
Almost certain	10	4.3%
Likely	16	7.0%
Possible	137	59.6%
Unlikely	56	24.3%
Highly unlikely	6	2.6%
Don’t know	5	2.2%

In these days of almost uncontrolled internet traffic of various types and equally frequent attacks on even highly protected countries’ defence systems, it is prudent to expect a major cyber threat at any time. Therefore, expecting at least one such major instance every year makes sense. It will enable us to prepare for such instances well in advance so that they can be prevented, managed with the least impact, or mitigated. Unfortunately, only <5% of the IT managers thought such a possibility to be certain. Overall, nearly 60% of IT managers thought that it was possible. Approximately 70% of all IT managers thought cyberattacks were possible or more than possible or more than possible. That leaves the rest, 30% of highly vulnerable firms, which is very serious.

Understanding Cyber Security

It should be noted that IT managers participated in this survey. So, they are expected to understand and explain the phenomenon of cyber security risks of various types. To what extent this is true is known from the data presented in Figure 4.

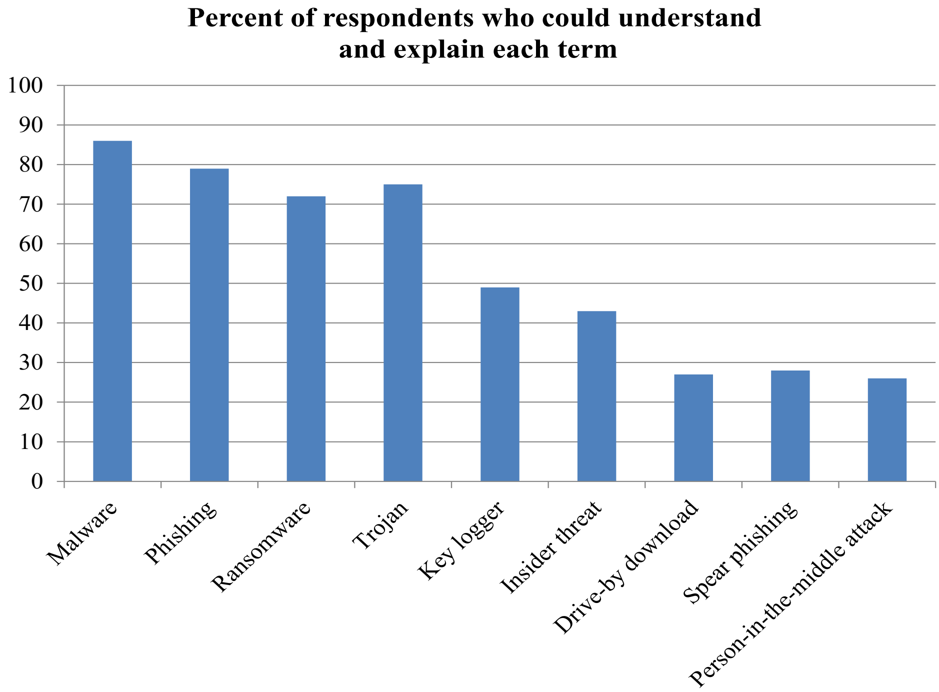

Figure 4. Percentage of survey respondents who understood and explained terms related to cyber threats

About 70–80% of the participants knew and could explain malware, phishing, ransomware, and Trojan, which are the most common types. Surprisingly, insider threat was known only to less than half of them. If an insider threat occurs in their own company, they may not be able to detect it and take countermeasures. These IT managers need to be educated and equipped to handle all types of cyber security risks to make them effective in their organisations.

DISCUSSION

Overall, in the case of Saudi private firms, there is much to be desired for near-perfect prevention/management of cyber-attacks in the future. Gaps were seen inadequate expenditure on cyber security even by high-income firms. Outsourcing may be a suitable strategy in many ways.

Equally, the security dimensions which can be outsourced and the parties to whom these are entrusted are critically important. Just to save money, outsourcing to unreliable parties may be self-defeating and even dangerous. Improvements in risk assessment are possible only if the current and future IT managers are equipped with the required knowledge and skills, which are highly inadequate at present.

One reason for this state of affairs may be awareness itself. In this study, the level of awareness, even among IT managers of private firms, was inadequate and quite serious in the case of certain types of security threats. There is a poor status of cyber security and its awareness at the public level, as was noted by Alarifi et al. (2012) through a survey. The highly censored, patriarchal, and tribal cultures were attributed as the reasons for the poor information security rating of the country. Even where awareness needs to exist at operational levels, intentional and deliberate security breaches of computerised accounting information systems (CAIS) could happen in Saudi organisations, as Abu-Musa (2006) reported. The types of security breaches identified were the accidental or intentional entry of bad data, accidental destruction of data by employees, unauthorised sharing of passwords among employees, the introduction of computer viruses to CAIS deliberately or accidentally, suppression and destruction of output; unauthorised document visibility and directing prints and distributed information to people who are not empowered to receive them.

A security culture should lead to sound information security management systems at the organisational level. Alnatheer and Nelson (2009) reported Saudi Arabian firms to lack in both these aspects. Although Saudi Arabia started promoting a National Commissions and IT Plan (NCITP) in 2005, cyber security does not find any place in that plan but only in the Ministry documents. Even in these documents, there is no adequate description of policies and strategies related to information security management. Security culture includes social, cultural, and ethical measures to improve the security-related behaviour by the organisational members as an organisational subculture. The earlier cited paper of Abu-Musa (2006) demonstrates the absence of such a culture in Saudi organisations. As measured by Hofstede (2019), the national cultural dimensions of Saudi Arabia show high power distance, uncertainty avoidance, and collectivism, which indicates that Saudi society is hesitant in adopting and implementing new practices that do not fit in their culture. As could be expected, Saudi organisations reflect the national culture. Overall, it means poor security culture and management in Saudi organisations (Alnatheer & Nelson, 2009).

In the studies of Alzamil (2018), most of the surveyed Saudi organisations had established an information security policy and deployed adequate levels of technology. However, ineffective and inefficient enforcement and publication and inadequate comprehensibility and clarity of these policies affected the level of cyber protection, even with the best systems. The use of the phrase ‘fair technology’ is important. These organisations did not have the best systems, but only good ones, which still provided enough room for malware attacks, affecting protection levels seriously. The results of this study also confirm these trends. Organisations are hesitant to spend money on cyber security and prefer to outsource a large part of their security components. In addition, IT managers are not adequately knowledgeable or equipped with risk assessment and analysis skills. These observations are borne out by the fact that, even after implementing information security and enforcement policies for data security management in many organisations, some critical issues were identified by Almutairi et al. (2020) for the attention of the national information security management authority.

According to the cyber security maturity model proposed in SAMA (2017), most Saudi organisations can be included in the first three levels (0,1,2) of non-existent, ad hoc, or repeatable but informal. These levels do not require high levels of knowledge. The observation of a low level of knowledge possessed by IT managers in this study is adequate for these three maturity levels. In a survey study of Saudi private organisations, similar to this study, Al-Harethi and Al-Amoodi (2019) observed that about 70% of IT managers were not aware of the security standards of Saudi Arabia. About two-thirds of the firms surveyed experienced different types of information security breaches. This finding reiterates the observation in the current study of poor risk perceptions of various types of cyber-attacks on their firms. Companies gave inadequate attention to proper security policy, access control, communications and operation management, personnel security, and organisational security. IT managers must explain these things to the top management.

Unfortunately, they lack awareness and knowledge on this subject. A strategy for business continuity management needs to be in place to restore economically important operations soon after any cyber-attack is countered. Outsourcing should be determined based on a risk assessment compared to internal development or different options of outsourcing. These findings support the observations of this study. The need for Saudi IT workers to develop their skills in many areas of cyber threat was noted by Al-Ghamdi (*In Press*). The gap in the knowledge between the Security Operation Team and other IT experts also needs to be narrowed down. This study showed that IT managers themselves do not have the required knowledge, narrowing the said gap will be a problem.

The findings point out the need to train the IT managers of Saudi private organisations on the possible cyber security breaches and the proactive strategies of protection and mitigating strategies when an attack occurs. IT managers need more than awareness to do their jobs effectively.

CONCLUSION

This study shows that Saudi private organisations do not invest adequately in cyber security. The tendency for outsourcing security management needs to be reviewed because of its risks. IT managers do not possess adequate knowledge or skills to anticipate the possibility of cyber-attacks and risk assessment procedures for proactive and mitigation strategies. They do not even possess the skills to identify internal security threats. Saudi private organisations need to take steps to rectify the organisational problems. IT managers can be sent to attend useful courses and workshops to acquire adequate knowledge and skills offered by various international organisations.

ACKNOWLEDGEMENT

The author wants to thank Umm Al-Qura University for the constant support and encouragement of research activities.

REFERENCES

Abu-Musa, A. A. (2006). Exploring perceived threats of CAIS in developing countries: The case of Saudi Arabia. *Managerial Auditing Journal, 21*(4), 387-407. https://doi.org/10.1108/02686900610661405

Ajmi, L., Alqahtani, N., Rahman, A. U., & Mahmud, M. (2019). A novel cybersecurity framework for countermeasure of sme's in saudi arabia. In *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-9). IEEE Publishing. https://doi.org/10.1109/CAIS.2019.8769470

Alarifi, A., Tootell, H., & Hyland, P. (2012). A study of information security awareness and practices in Saudi Arabia. In *International Conference on Communications and Information Technology (ICCIT)* (pp. 6-12). IEEE Publishing. https://doi.org/10.1109/ICCITechnol.2012.6285845

Al-Ghamdi, M. I. (In Press). Effects of knowledge of cyber security on prevention of attacks. *Materials Today: Proceedings*. https://doi.org/10.1016/j.matpr.2021.04.098

Al-Harethi, A. A., & Al-Amoodi, A. H. (2019). Organisational factors affecting information security management practices in private sector organisations. *International Journal of Psychology and Cognitive Science, 5*(1), 9-23.

AlMindeel, R., & Martins, J. T. (2020). Information security awareness in a developing country context: insights from the government sector in Saudi Arabia. *Information Technology & People, 34*(2), 770-788. https://doi.org/10.1108/itp-06-2019-0269

Almutairi, M. M., Halikias, G., & Yamin, M. (2020). An overview of security management in Saudi Arabia. In *7th International Conference on Computing for Sustainable Global Development (INDIACom)* (pp. 261-265). IEEE Publishing. https://doi.org/10.23919/INDIACom49435.2020.9083725

Alnatheer, M., & Nelson, K. (2009, December 1-3). Proposed framework for understanding information security culture and practices in the Saudi context. In *Proceedings of the 7th Australian Information Security Management Conference* (pp. 6-12). Queensland University of Technology, Perth, Western Australia. https://doi.org/10.4225/75/579850d331b4d

Alotaibi, F. F. (2019). *Evaluation and enhancement of public cyber security awareness* (PhD Thesis). University of Plymouth, England. https://pearl.plymouth.ac.uk/bitstream/handle/10026.1/14209/2019ALOTAIBI10392328PhD.pdf?sequence=1

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A survey of cyber-security awareness in Saudi Arabia. In *11th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 154-158). IEEE Publishing. https://doi.org/10.1109/ICITST.2016.7856687

Alshammari, T., & Singh, H. (2018). Preparedness of Saudi Arabia to defend against cyber crimes: An assessment with reference to anti-cyber crime law and GCI index. *Archives of Business Research, 6*, 131-146. https://doi.org/10.14738/abr.612.5771.

Alsmadi, I., & Zarour, M. (2018). Cybersecurity programs in Saudi Arabia: Issues and recommendations. In *1st International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-5). IEEE Publishing. https://doi.org/10.1109/ICIT52682.2021.9491711

Alzahrani, A., & Alomar, K. (2016). Information security issues and threats in Saudi Arabia: A research survey. *International Journal of Computer Science Issues, 13*(6), 129-135. https://doi.org/10.20943/01201606.129135

Alzamil, Z. A. (2018). Information security practice in Saudi Arabia: Case study on Saudi organisations. *Information & Computer Security, 26*(5), 568-583. https://doi.org/10.1108/ICS-01-2018-0006

Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon, 7*(1), Article e06016. https://doi.org/10.1016/j.heliyon.2021.e06016

Basamh, S. S., Qudaih, H. A., & Ibrahim, J. B. (2014). An overview on cyber security awareness in Muslim countries. *International Journal of Information and Communication Technology, 4*(1), 21-24.

Elnaim, B. (2013). Cyber crime in Kingdom of Saudi Arabia: The threat today and the expected future. *Information and Knowledge Management, 3*(12), 14-19.

GMI. (2021). *Saudi Arabia social media statistics 2021.* Global Media Insight. https://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics/

Hawdon, J. (2021). Cybercrime: Victimization, perpetration, and techniques. *American Journal of Criminal Justice, 46*, 837-842. https://doi.org/10.1007/s12103-021-09652-7

Hofstede, G. (2019). *National culture*. Hofstede Insights. https://www.hofstede-insights.com/models/national-culture/

Hydrocarbon Processing. (2020). *Saudi Aramco sees increase in attempted cyber-attacks.* Hydrocarbon Processing. https://www.hydrocarbonprocessing.com/news/2020/02/saudi-aramco-sees-increase-in-attempted-cyber-attacks#:~:text=Aramco%2C%20which%20pumps%2010%25%20of,at%20the%20biggest%20OPEC%20exporter

ITU. (2021). *Measuring digital development facts and figures 2021.* International Telecommunication Union. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2021.pdf

Perlroth, N., & Krauss, C. (2018, March 15). *A cyberattack in Saudi Arabia had a deadly goal. Experts fear another try.* The New York Times: https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html

Quadri, A., & Khan, M. K. (2019). *Cybersecurity challenges of the Kingdom of Saudi Arabia: Past, present and future*. Global Foundation for Cyber Studies and Research.

SAMA. (2017). *Cyber security framework.* Saudi Arabian Monetary Authority. https://www.sama.gov.sa/en-US/Laws/BankingRules/SAMA%20Cyber%20Security%20Framework.pdf

Stock, J. (2020). *INTERPOL report shows alarming rate of cyberattacks during COVID-19.* Interpol. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Talib, A. M., Alomary, F. O., Alwadi, H. F., & Albusayli, R. R. (2018). Ontology-based cyber security policy implementation in Saudi Arabia. *Journal of Information Security, 9*(4), Article 88030. https://doi.org/10.4236/jis.2018.94021

The Global Statistics. (2022). *Saudi Arabia social media statistics 2021: Internet & mobile statistics.* The Global Statistics. https://www.theglobalstatistics.com/saudi-arabia-social-media-users/

Wright, B., & Allan, K. (2020). *Saudi CIOs consider security their toughest tech challenge.* IDG Communications Inc. https://www.cio.com/article/3445225/saudi-arabias-cybersecurity-concerns-increase-as-threats-evolve.html