An Overview of Cyber-Security Awareness In Saudi Arabia: The Threat Today and the Expected Future

Mishaal Almutairi

Mishaal.motary@gmail.com

Lecturer at Majm'mah technical college (MJCT)

Abstract

In 2012, the official King Saud University's website was hacked and database of 812 users exposed including mobile phones, mail address and passwords. In 2013, several Saudi Arabia government websites were hacked in a series of sabotage cyber-attacks briefly disabling them before the threats were repelled. On 15th August 2012, a self-replicating virus attacked over 30000 Windows OS based personal computers belonging to Saudi Aramco deleting data and information. It took two weeks and unfathomable losses to restore the data. Multiple research findings, articles and academic papers document cyber-attacks threatening security across the world. Both the government and private enterprises are targets of cyber-attacks. The threats are more pronounced with increased reliance on information technology and heightened e-government pedagogy. Following recent cyber-attacks, this paper digs deep to review the forms of cyber-attacks, the private and publics' awareness of cyber-security threats, potential impacts of cyber-attacks, measures enacted to fight cyber-attack and recommendations to help raise awareness. Data gathered will be analyzed using SPSS 2.0 software and presented in tables, pie charts and graphs. The researcher will calculate standard deviation, percentages. The researcher envisages that at the end of the survey, the paper will document an indispensable roadmap for policy makers in Saudi Arabia in designing measures to mitigate future cyber-attacks to both the private and public in the kingdom.

Keywords: Cybersecurity, cyber-attacks, Saudi Arabia, information security.

1 Introduction

The preceding decade has seen an unprecedented rise in the volume and severity of cyber-attacks around the world, with some of the attacks such as 'Stuxnet' and 'LulzSec' gaining such widespread notoriety that they almost became part of common vernacular. As modern-day organisations place an ever-increasing amount of business-critical information in network-accessible locations, the spectre of cyberattacks has become a very credible threat.

Several international sources have noted that Saudi Arabian businesses are particularly vulnerable to cyber-attacks due to a lack of technical standards or regulatory bodies to oversee the introduction of security measures. A recent incident where the IT infrastructure of state oil company Aramco was attacked by malicious entities, resulting in the loss of substantial amounts of information, appear to indicate there might be some truth to this hypothesis. In this paper, the levels of organisational awareness relating to cybersecurity in Saudi Arabia and the potential threat from these attacks will be critically analysed.

2 Literature Review

While the Middle East as a region constitutes only 3.2% of the world's population of internet connected users, the region has seen internet usage grow by 1825% over the past 10 years, compared to 445% for the world as a whole (Aloul, 2012). Saudi Arabia is the largest country in the Middle East in terms of GDP, and has seen the volume of online business increase by 14.3% over the previous year (World Bank, 2015).

Concurrently, the number of cyber-attacks has increased substantially in the same timeframe; with Burg et al (2014) noting that the number of attacks across the world had risen by 63% between 2013 and 2014 alone. That year, 5 out of every 6 large organisations experienced some form of cyber-attack at least once.

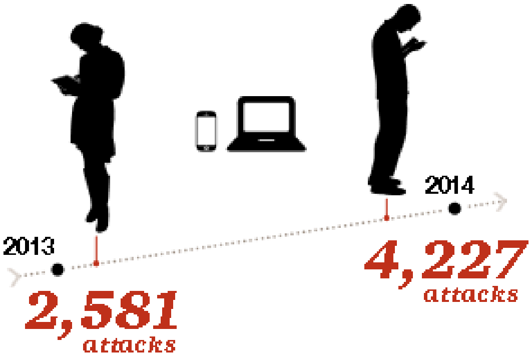


Fig. 1: Increase in no. of cyber-attacks, 2013-2014

The Saudi government has recognized the threat posed by cyberattacks to the Saudi economy which is comprised largely of public-sector corporations; the Ministry of Communication and Information Technology (2015, pg. 79) notes: “Cybersecurity is the newest and unique national security issue of the 21st century. Every day Gulf Cooperation Council businesses are targeted for cyber exploitation and theft. This consistent and extensive cyber looting results in huge losses of valuable intellectual property, sensitive information, and jobs for the Kingdom. Without an immediate initiative to develop and implement a cybersecurity policy, the Kingdom will continue to be at risk for a catastrophic attack to the nation’s vital networks – networks that power essential services for continuity of national security operations and economic stability.”

Recent events would appear to verify this alarming prediction; the first high-profile attack was on the Riyadh Bank in June 2010, where several customers had the balances of their accounts erased. This was followed by an attack in December 2011, where the Wiper malware was used to successfully erase information on the Saudi Oil Ministry’s hard drives (Al-Arifi et al, 2012).

However, both of the above paled in comparison to the “Shamoon” attack in 2012 where 30,000 Windows workstations at Saudi Aramco were taken down by the eponymous virus; the organisation spent more than a week restoring the systems to operation. Following this, another attack in October 2013 took down multiple Saudi government websites for a span of several hours. Among the casualties was the website of the interior ministry – responsible for security – which broke down under the volume of millions of bogus requests in a denial of service attack (Reuters, 2013).

An analysis of contemporary literature on the root cause of these cybersecurity vulnerabilities reveals some consensus. In an analysis of cyber-attacks specific to Middle-Eastern countries, Al-Gahtani et al (2007) postulated that despite the introduction of anti-cybercrime laws in 2006, Saudi Arabia suffered from continued cyber-security attacks because of a lack of awareness amongst residents of such cybercrime laws, lack of IT knowledge on the part of law enforcement officials, and an absence of cybersecurity experts amongst the Saudi workforce. Similarly, Kalabasi et al (2012) identified 7 different reasons why GCC nations were so vulnerable to attack, and noted that the two most significant were limited IT-security knowledge amongst users who were targeted as the “weakest link”, and limited enforcement or scope of cybercrime laws.

The United Nations ITU (2015, pg. 1) notes in its cyber-wellness report that one of the issues with cybersecurity in the Kingdom is that there exist no frameworks for cybersecurity that allow for the accreditation or certification of either organisations or professionals in the Saudi Arabia.. It therefore becomes imperative to ascertain to what extent these theoretical hypothesis translate into actual cybersecurity threats in practice, and whether the lack of awareness leads to real vulnerabilities.

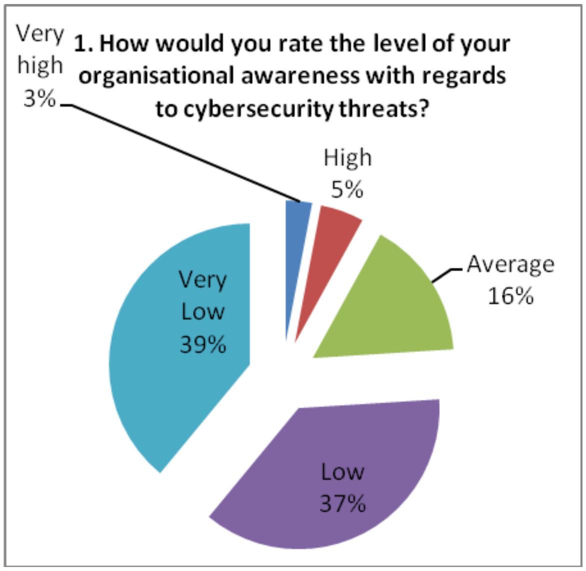
3 STUDY METHODOLOGY

The study was conducted on 266 information technology professionals from Saudi Arabia; the means of distribution was mostly online through the survey panel platform Question Pro. The panel restricted the survey to respondents whose job function was Information Technology and who held a managerial, senior, mid-level or technical position within their organisation.

According to the MCIT (2015), there are approximately 20,000 individuals who work directly in information technology in Saudi Arabia; at a population of this size, a sample of 266 at the 95% confidence level (i.e. 2 standard deviations from the mean) would give a confidence interval of approximately 5 standard deviations at the most even percentage split, i.e. the upper and lower ranges for each response would be within 5% of the mean for the population. This can be considered a statistically significant response, according to Malhotra (2009).

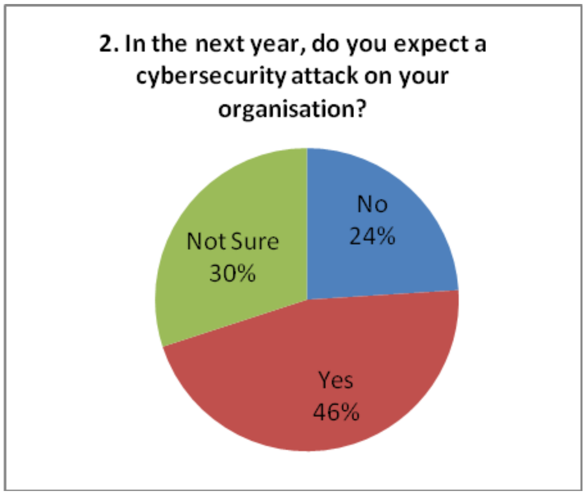
4 RESULTS AND ANALYSIS

Question 1 in the survey asked the respondents to rate the awareness of their organisation as a whole in regards to cybersecurity and the threats it may pose.

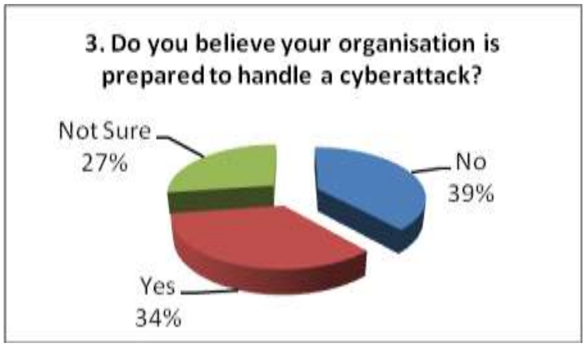


The majority (76%) of respondents ranked their firm’s organisational awareness as either ‘low’ or ‘very low’; only a combined 8% ranked awareness as ‘high’ or ‘very high’. From the onset this would suggest that Saudi organisations do have a problem with cybersecurity awareness.

The second question sought to find out the likelihood of a cybersecurity threat in the next year as an indicator of the severity and immediacy of the problem. 46% of the respondents felt an attack was imminent, which represents the largest proportion of the responses.

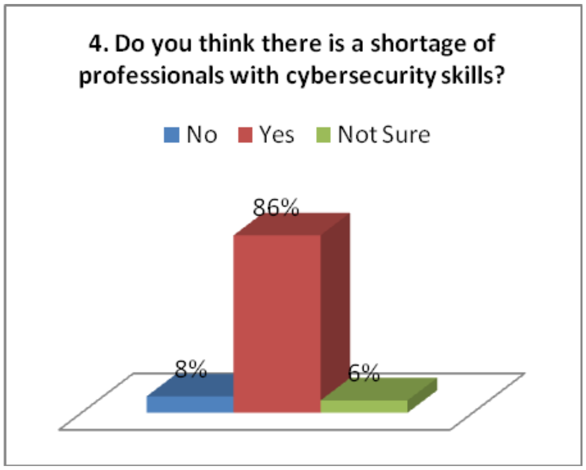


The third question asked the respondents if they felt their organisation was adequately equipped to handle a cyberattack should the eventuality occur.



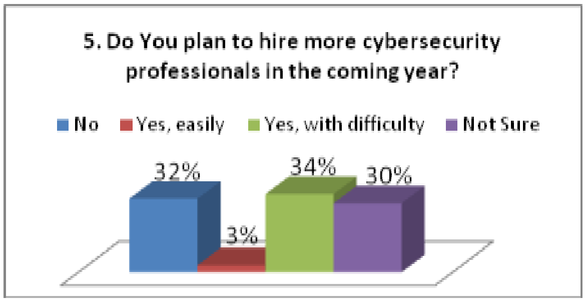
Only 34% of the respondents felt that their organisation was adequately equipped to handle the attack, with the rest either unsure or not confident.

The fourth question asked respondents if there was a shortage of professionals that could advise Saudi organisations on cybersecurity best practice.



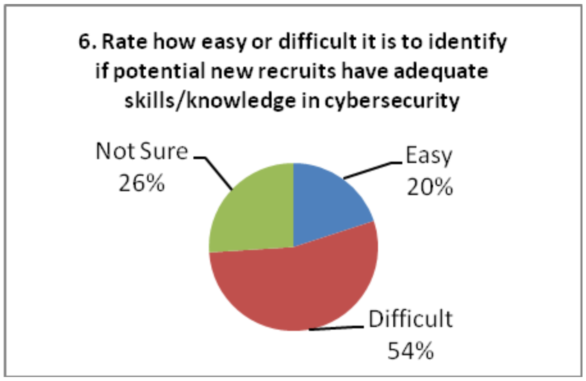
The vast majority (86%) of respondents – who as managers would have a stake in the hiring process – felt that there was a shortage of cybersecurity skills in the Saudi IT industry.

Question 5 asked respondents if they planned to hire cybersecurity professionals, with the positive response split to further reflect how easy they thought this process might be.



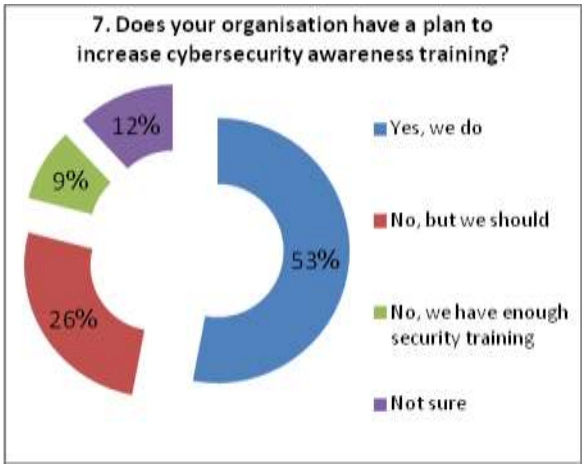
34% of the respondents reported that although they would like to hire more professionals, they felt this would be a difficult process. Only 3% thought the process would be easy, while 30% were not sure if they would hire more professionals.

Question 6 concerned the awareness and suitability of new IT recruits in handling cybersecurity threats; given the heightened profile of cybersecurity in recent years the question arose if newer recruits would be the answer for handling such threats.



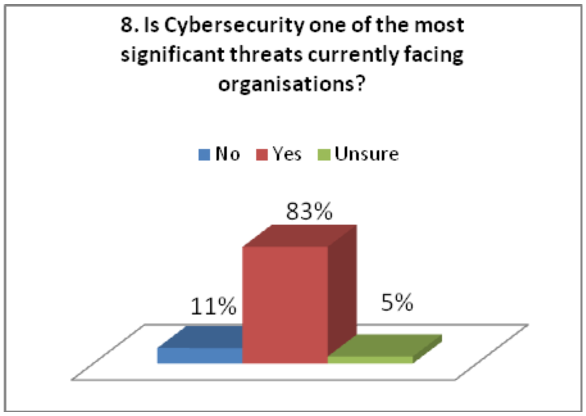
The issue is that the majority of current IT managers (54%) are unable to identify if recruits will be able to handle cybersecurity threats or not; only 20% of the respondents felt it was easy to pinpoint a recruit’s cybersecurity awareness.

Given that current awareness and readiness levels were so low, the next question sought to find out if there were training programmes in place to remedy this.

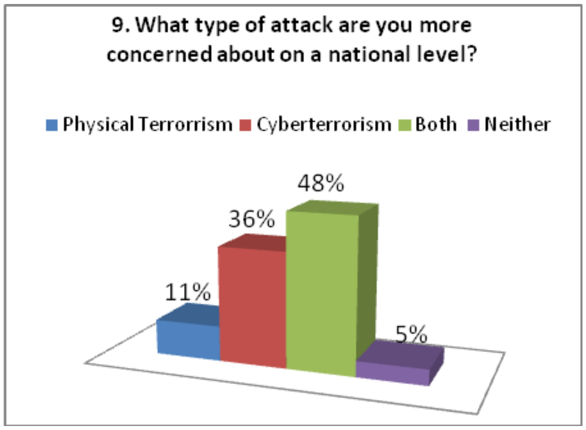


53% of the respondents had plans in place to increase cybersecurity awareness; of the remainder, the majority (26% of total) felt that although the organisation didn't have plans in place, it was necessary. Only 9% felt there was enough training in place.

Question 8 asked respondents to rate the significance of the cybersecurity threats. The vast majority (83%) rated cybersecurity as one of the most significant threats the organisation faced.

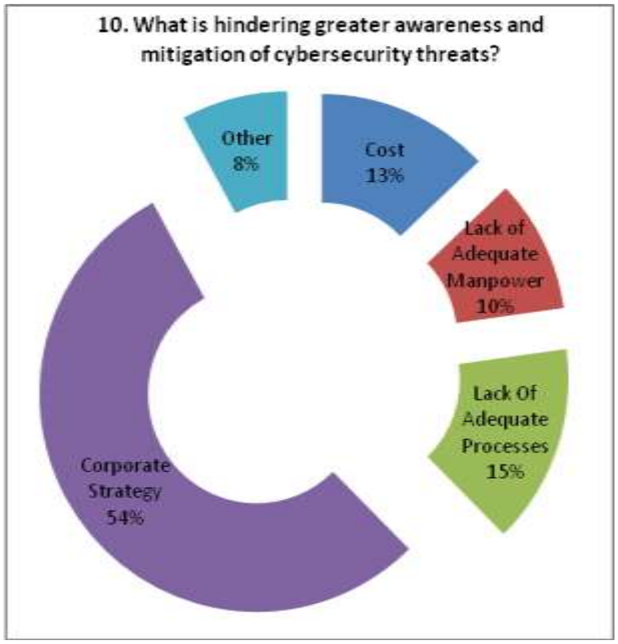


Similarly, question 9 asked respondents about cybersecurity at the state level, vis-à-vis physical threats such as terrorism.



While 36% of respondents rated cyberterrorism the most significant threat, 48% responded that they were equally concerned about cyberterrorism and physical terrorism. This indicates that the majority of respondents are concerned about the threat of cyberterrorism to the Saudi nation.

The final question asked respondents of what they rated as the biggest hindrance to awareness/mitigation of cybersecurity threats.



The majority (54%) felt that there was a lack of strategy to combat cyberattacks at the organisational level; a further 15% felt that there were inadequate processes in place.

5 SUMMARY AND RECOMMENDATIONS

The results of the survey analysis effectively bear out what has been cited by numerous professionals and academics in the literature – that cyber-attacks present a real, imminent and severe threat to the security of organisations in Saudi Arabia. The majority of the survey respondents agreed that cybersecurity was perhaps the most critical threat that organisations currently faced more so than physical terrorism – and almost half expected to face an attack within the next year.

The awareness of such attacks is a real problem for IT managers and teams in the country; as mentioned by NIST (2007), cybersecurity should be a concern for every person in the organisation, yet the survey found that more than three quarters of the organisations surveyed had low to very levels of cybersecurity awareness. The majority of those surveyed also stated that it was difficult to find adequately-trained professionals to handle cybersecurity threats, and that it was difficult to find new recruits who could be appropriately trained to do so.

Ultimately, what can be inferred from the survey results with context from the secondary research is that mitigating the risks from cybersecurity will require a serious change in corporate culture, and a greater investment in training for cybersecurity at the national level from the government and authorities.

The following recommendations are issued on the basis of the research:

1. Organisations are in urgent need of training in order to increase employee awareness of cybersecurity threats.

2. The government and educational authorities need to implement strategies to include cybersecurity awareness amongst future employees.

3. More needs to be done to handle cybersecurity at a national level, such as perhaps an oversight body or a set of standards for best-practices implementation.

REFERENCES

Al-Arifi, A., Tootell H.and Hyland, and P. (2012) “Information Security Awareness in Saudi Arabia”, In: Proceedings of the CONF-IRM 2012, Wollongong: Australia
Al-Gahtani, S.S., Hubona, G.S. and Wang, J. (2007) “Information technology (IT) in Saudi Arabia: Culture and the acceptance and use of IT”, Information & Management, Vol. 44 No. 8, Pg. 681-691
Aloul, F.A. (2012) “The Need for Effective Information Security Awareness”; Journal of Advances in Information Technology, Vol. 3 No. 3, Pg. 176-184
Anon. (2015) “Developing National Information Security Strategy for the Kingdom of Saudi Arabia”, Riyadh: Ministry of Communication and Information Technology
Burg, D., Loveland, G. and Cornell, T. (2014) “Cyberattacks on the rise: Are private companies doing enough to protect themselves?”, New York: Price Waterhouse Coopers
ITU (2015) “Cyber-Wellness Profile for Kingdom of Saudi Arabia”, Geneva: United Nations
Kalbasi, A., Alomar, O., Hajipour, M. and Aloul, F. (2012) “Wireless security in UAE: A survey paper”, in: Proceedings of the IEEE GCC Conference 2012, Dubai: UAE
Malhotra, N.K. (2009) “Marketing Research: An Applied Orientation”, Upper Saddle River: Prentice Hall
Reuters (2013) “Saudi Arabia Faces Major Cyber Attack”, Gulf News, Issue: 18 May 2013
World Bank (2015) “World Development Indicators: 2015”, Washington D.C.: World Bank