A Review of Cybersecurity in the Saudi Arabian Context

Sultan Rashed Aldosari

University of Bedfordshire, UK

Abstract

A systematic review of available literature was conducted on the topic of 'Cybersecurity in the Saudi Arabian Context'. A search protocol was devised and relevant search terms were input in to the Google Scholar open source search engine. Around 210 scholarly and research works were considered before five were chosen for further analysis. These works were chosen keeping the topic of enquiry in mind and with an aim towards choosing only recent works. The five shortlisted works were studied and analysed further in order to glean some important observations on the state of enquiry into the aforementioned topic of cybersecurity in the Saudi Arabian context. It was concluded that research existed on cyber threats at three levels; one, at the level of crimes against the general public, two, threats to companies and three, threats to the national infrastructure. It was also evident from conducting the systematic review that there was not adequate research on the topic and many avenues for further scientific enquiry exist.

Keywords: Cybersecurity, Saudi Arabia, Cyber Attacks, Challenges, Review

Introduction

As information and communication technology (ICT) has evolved, so too has the use of it in essential services around the world. Computer technology is now used in nearly every aspect of life in the world today; therefore cyberspace has also become a new frontier that is rife with criminality and attempts by criminal elements to use information in this realm in order to attack or cheat others. As a result, threats on cyberspace have escalated across the globe. Thus, the birth of cybersecurity, i.e. the protection of information and data in the online realm, has taken place and proliferated at the international level.

The aim of this article is to focus specifically on the issue of cybersecurity in the context of the Kingdom of Saudi Arabia. In order to do so, a systematic review was conducted to find relevant literature in this field, thereby finding some aspects of cybersecurity in the country, including the challenges being faced and strategies being used to counter cyber-attacks.

A search was conducted on the open source search engine of Google Scholar, and relevant research and scholarly works were found. Using criteria that are outlined further in following sections, the articles were narrowed down to a manageable number in order to be analysed further. The observations found from these articles were discussed further in the final section of the article.

Cybersecurity in Saudi Arabia

The Kingdom of Saudi Arabia has a high level of penetration of information and communication technology, including mobiles phones and broadband connections. The internet was introduced to the country in 1994. (Hathaway, Spidalieri, & Alsowailm, September 2017)

According to one estimate, there are 69.6 internet users for every 100 persons in Saudi Arabia, which has a total population of over 31.5 million. Mobile phone subscriptions, on the other hand,

are at 177 connections for every 100 persons, at a penetration rate of 177%. (Hathaway, Spidalieri, & Alsowailm, September 2017)

The country, as well are other neighbouring countries in the Middle East, are at risk for cyber threats. In 2018, analysts warned that cyber attacks in the Gulf countries were a growing threat to businesses operating in the region. Analysts even pointed to the fact that the cost of data breaches had grown significantly in 2017 for countries in the region. It was also mentioned that despite Saudi Arabia's proactive steps, such as setting up a National Authority for Cyber Security, the threats could not be wholly curbed, and that for Saudi Arabia specifically, the re-emergence of a virus that caused a major issue in 2012, i.e. the Shamoon Virus, was a threat. (Spong, 2018)

However, the threats go beyond risk to businesses, according to some reports. An attack prevented in 2017 was not only designed to attack the data of a petrochemical plant in Saudi Arabia, but was actually designed to trigger an explosion. (Perlroth & Krauss, 2018)

There have previously been some major attacks on Saudi critical infrastructure through the means of cyber threats, such as the aforementioned Shamoon virus that threatened Saudi Arabia's Aramco, which managed to shut down the world's largest oil and gas company and cause significant damage. Moreover, as part of the country's Vision 2030, there have been steps to address cybersecurity threats. (Hathaway, Spidalieri, & Alsowailm, September 2017)

Review

In order to find relevant literature, the open source engine, Google Scholar was used. Google Scholar reveals only those works marked as scholarly articles when specific search terms are entered into it. Moreover, it shows scholarly works stored in many different scholarly databases, thereby widening the number and types of articles that can be searched for.

First, a number of relevant search terms were conceptualized to enable finding the most relevant scholarly works. These search terms or phrases were intended to be entered into the Google Scholar search engine. These search phrases are listed below.

- Cyber Security in Saudi Arabia
- Cybersecurity in Saudi Arabia
- Strategies for Cybersecurity in Saudi Arabia
- Cyber Attacks in Saudi Arabia
- Cyber Security in Arab Countries
- Cyber Threats in Saudi Arabia
- Cyber threats in Arab Countries

Once these search terms were entered into the search engine, each search term produced hundreds of results, with each page of results containing ten scholarly works. Due to the constraints of writing a brief review article, only five articles were chosen to be analysed further. For each search term, no more than the first three pages of results were looked into. Thus, for the seven search terms, with three pages of results for each term and ten results per page, a total of 210 articles were considered in total. The issue of cybersecurity is still an emerging one, care was taken to choose articles from recent years in order to present more up-to-date research and analysis.

Each of the five articles chosen are listed below and some important details about each work is presented alongside the articles.

1. The first work is entitled, 'Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future' and was written by author Bushra Mohamed Elamin Elnaim from the Department of Computer Science and Information at the College of Science and Humanity Studies-Alsulial in Salman Bin Abdulaziz University in Saudi Arabia. This work discusses the different types of cybercrime, such as hacking, dissemination of viruses, denial of service attacks, phishing, spamming, cyber stalking, and cyber terrorism. The aim of the article is to not only discuss cybercrime and its proliferation in Saudi Arabia, but to also discuss the response from the Saudi Arabian government, specifically to do with the types of legal responses that have been drawn up, such as the IT Act, which helps the state deal with such crimes. The author not only details the high rate of internet penetration in Saudi Arabia, and the resulting increase in cyber crime, but also points to studies that have shown that cyber crime in the Kingdom of Saudi Arabia had cost the country around SR 2.6 billion in the year 2012. The author also outlines the new IT Act, the Arab Cyber Crime Agreement of 2012, which addresses credit card frauds, internet crimes, cyber terrorism, creation and/or distribution of viruses, hacking, system interference, and illegal access and interception, amongst others. The author concludes that the issue is an ongoing one, and the prevention of cyber crime will remain a challenge for the country. (Elnaim, 2013)
2. The second work is by authors Salem Alelyani and Harish Kumar GR from King Khalid University in Saudi Arabia entitled, 'Overview of Cyberattack on Saudi Organizations'. The authors not only discuss in the increasing pace of cyber crimes, but also specifically discuss how countries exploit vulnerabilities in cybersecurity in other countries in order to gain an advantage or upper hand. In this regard, the authors contend that developed countries have done the most to exploit the cyber-vulnerabilities of other countries. The authors also point to malware, also known as malicious software, as a major security threat in the cyber realm. In discussing the context of Saudi Arabia, the authors believe that the Kingdom has become a major target for cyber threats due to increased economic activity, digital transformation, a relatively high rate of adoption of technology and the rise of the oil and gas industry. On the other hand, the authors also believe that there hasn't been enough scientific research into the cyber threats faced by Saudi Arabia, leading the authors to present their research in this context. The authors focus on two specific malware, Shamoon and Ransomware and the timeline of attacks that have taken place in Saudi Arabia. Ultimately, according to the authors, their aim is to outline how the country may be able to protect itself in the future. (Alelyani & Kumar, 2018)
3. The third work is entitled, 'Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident' and was written by authors Zakariya Dehlawi and Norah Abokhodair. As the title suggests, the authors focused on one major cyber attack that took place in Saudi Arabia as a means of presenting their research. The authors frame their research as a progress report of cybersecurity at large companies, and the importance of cybersecurity in the financial as well as operational capacities of the companies. For their research, the authors focused on Saudi Aramco, the state-held oil company that is also the largest in the world. In 2012, the company was targeted in a massive cyber attack that not only paralyzed their operations, but also had major, long-lasting impact on the company's ability to function for months after the initial attack. The authors analysed the response of

Aramco to the attack, as well as its present-day policies in the field of cyber threats and responses. In particular, the authors focused on how the government of the Kingdom of Saudi Arabia responses to the attack and how the country's response might fare under current cybersecurity benchmarks and standards. (Dehlawi & Abokhodair, 2013)

4. The fourth paper was published by the Potomac Institute for Policy Studies. Written by authors Melissa Hathaway, Francesca Spidalieri, and Fahad Alsowailm, the paper entitled, 'Kingdom of Saudi Arabia: Cyber Readiness at a Glance', delves into the readiness of the Kingdom of Saudi Arabia in its ability to ward of cyber threats. The authors detail the country's information and communication technology status, including the level of mobile and internet penetration in the country. The authors also detail the country's government strategy in dealing with cyber attacks, including outlining the National Information Security Strategy and Vision 2030 and how these national actions may deal with cyber threats. According to the authors, in 2017, a series of royal decrees were issued that established a Presidency of State Security, repositioning the National Cyber Security Center under the Presidency to become the focal point for cyber security in the Kingdom, thereby focusing the strategy and response to a single entity. The authors delve into the history of cyber security in the country as well as outlining the types of threats faces until the year 2017, as well as the responses to those incidents. Apart from this, the authors also look at the realm of e-crime or cyber crime and the responses of law-enforcement officials in the Kingdom of Saudi Arabia to the same. The authors also looked at other aspects of cybersecurity, such as information sharing and research and development of tools. In conclusion, the authors believe that the Kingdom of Saudi Arabia is, unfortunately, still insufficiently prepared for its cybersecurity, despite making remarkable progress in becoming more cyber ready. (Hathaway, Spidalieri, & Alsowailm, September 2017)
5. The final paper is entitled, 'A study of information security awareness and practices in Saudi Arabia' and was written by authors Abdulaziz Alarifi, Holly Tootell and Peter Hyland. This work approaches the issues of cybersecurity from the point of view of awareness of issues amongst the general public and what might challenge broader awareness of information security in the country. The authors contend that awareness of information security threats is very poor in Saudi Arabia, especially in comparison to countries in the West. The authors state that this is the case despite the widespread use of internet through mobile phones, apps and other means of communication and usage. The authors used an anonymous online survey on the issue of information security awareness (ISA) created by Malaysian Cyber Security Organization and company KPMG. In total, around 633 respondents answered the survey. The results showed the authors that information security awareness in Saudi Arabia is quite low. The authors attribute this low level of awareness to the high level of censorship within the country, as well as the tribal and patriarchal nature of the country's society. (Alarifi, Tootell, & Hyland, 2012)

Some of the observations gleaned from these papers and the analyses of the same will be further discussed in the following section.

Discussion and Conclusion

The most striking observation from conducting the search and analysing the results was the fact that there is a significant dearth of scholarly work and scientific exploration on the subject of cybersecurity threats in the country of Saudi Arabia.

In the search stage, it was a struggle to find papers that had specifically to do with this issue and to do with the specific geography of the country of Saudi Arabia. It bears mentioning that there were some other papers that actually discussed broader issues, or other countries, that also mentioned the issue of cybersecurity in Saudi Arabia, but only as part of a larger topic or regional discussion.

As mentioned in the second paper analysed, this lack of scientific study on this topic is a hindrance and needs to be corrected.

As the research works showed, there are a few different levels at which cybersecurity is threatened in Saudi Arabia. One, at the level of general public, almost all of whom have access to the internet in some form or the other in Saudi Arabia. The fifth and final paper revealed that information security awareness is low in the country, leading its citizens to be susceptible to threats to their personal data. The second is at the level of companies which can have their data breached or their operations attacked in other ways. This type of attack was discussed in some way, shape or form by the first three papers. The third is at the level of attacking national infrastructure with an aim to causing national damage or taking lives. This can be called cyber terrorism and was addressed in the first, third and fourth paper. In the third paper, though the attack on Aramco can be considered an attack on the company, the significance to the national economy of Saudi Arabia and the amount of damage that was caused, it could also be considered an attack on the country.

As the first and the fourth papers detailed carefully, there is evidence that there has been a growing response and strategy from the country, in the form of dedicated response agency to the issue of cyber threats and necessary legislation. However, according to the authors of the fourth paper, despite the progress, there is still a lack of readiness to address cyber threats in the Kingdom of Saudi Arabia.

It is evident from conducting this review that there are several avenues for further research, especially as detailed previously, there has not been enough scientific enquiry in this field. For one, cyber threats against Saudi Arabia need to be quantified better, in more details and sorted by type of threat, size of threat, etc. Apart from this, while there have been some papers looking into Saudi Arabia's cyber readiness, including some of the papers outlined in this review, there still needs to be more research done in this area, especially from different points of view. This could be from the point of view of the general public, smaller companies, large nationalized companies, and finally from government agencies. It is clear that since the attack on Aramco, there has been a considered government response, but how this response compares with the response of other countries, what lessons can be transplanted to the Saudi context from other countries, and what gaps exist in the responses, are all areas that require further exploration, scientific scrutiny and scholarly pursuit.

References

Alarifi, A., Tootell, H., & Hyland, P. (2012). A study of information security awareness and practices in Saudi Arabia. *2012 International Conference on Communications and Information Technology (ICCIT).* Hammamet, Tunisia: IEEE.

Alelyani, S., & Kumar, H. (2018). Overview of Cyberattack on Saudi Organizations. *Journal of Information Security and Cybercrimes Research (JISCR).*

Dehlawi, Z., & Abokhodair, N. (2013). Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident. *2013 IEEE International Conference on Intelligence and Security Informatics.*

Elnaim, B. M. (2013). Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future. *Information and Knowledge Management, 3*(12).

Hathaway, M., Spidalieri, F., & Alsowailm, F. (September 2017). *Kingdom of Saudi Arabia: Cyber Readiness at a Glance.* Arlington, Virigina, United States of America: Potomac Institute for Policy Studies.

Perlroth, N., & Krauss, C. (2018, March 21). *A cyber attack in Saudi Arabia failed to cause carnage, but the next attempt could be deadly.* Retrieved from The Independent: https://www.independent.co.uk/news/long_reads/cyber-warfare-saudi-arabia-petrochemical-security-america-a8258636.html

Spong, R. (2018, March 26). *Cyber attacks a 'real threat' to Gulf business.* Retrieved from Arab News: http://www.arabnews.com/node/1274021/business-economy