ISSN:0975-9646

Why Cybersecurity Awareness is Essential

Yasir Bangash / Ahmed Bahaitham / Ehab Saggaf

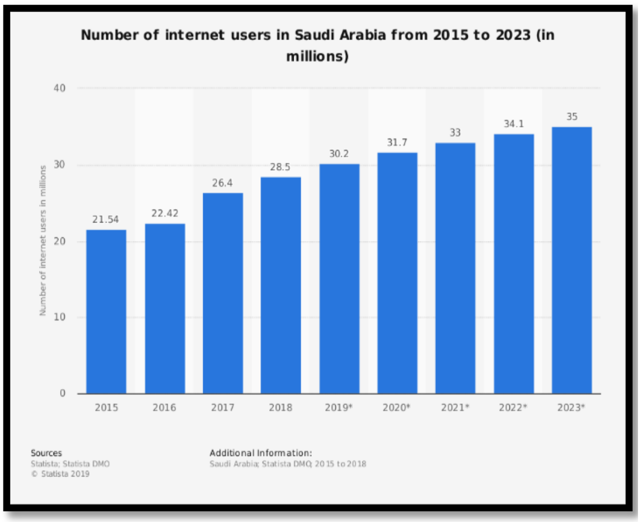
IT Department, Saudi Aremco

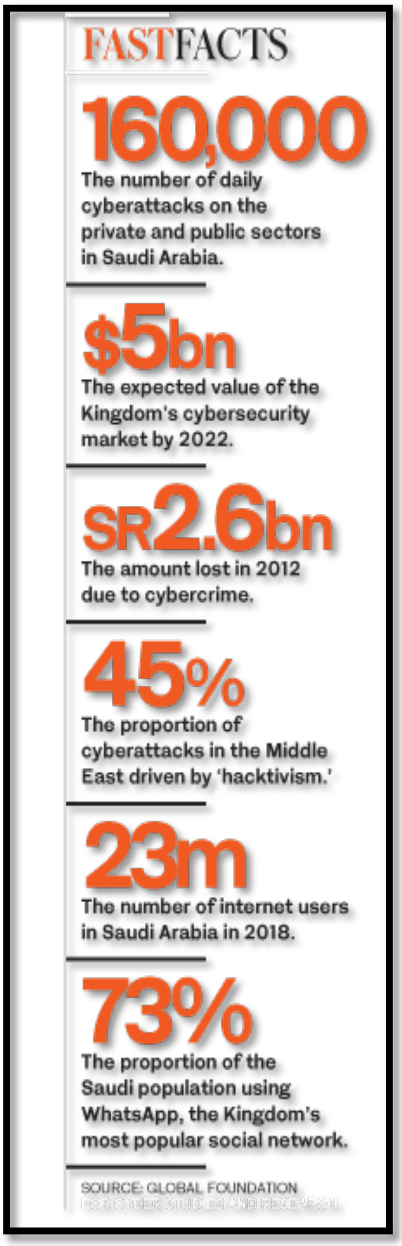
***Abstract*-Cybersecurity awareness is crucial in helping to prevent cyber-attacks on private sector companies, especially with the increased use of social networking applications. Saudi Arabia is one of the fastest developing countries in the Middle East, where the uptake of communication technologies, such as the internet and mobile technologies, has risen sharply in recent years, as the number of internet users rose from 21.5 million in 2015 to 31.7 in 2020 [1]. These technologies are relatively new to the region. Therefore, the crimes associated with these technologies are also new to the people in the region. This article studied and analyzed the level of Information Security awareness for private sector companies in Saudi Arabia for the last five years. In addition, the study provided recommendations to improve the cybersecurity awareness, which will improve the overall information protection for these companies. Due to the intricacies of the internet, the level of awareness has an influencing impact on the companies. Thus, to ensure private sectors can fend off cyber-attacks and have safe networks, it is necessary to safeguard the network. A newly published report by Symantec has revealed that 69% of Saudi companies cannot cope with cyber-attacks due to the lack of cybersecurity awareness programs and training for their employees. [2]**

Keywords: Cybersecurity Awareness, Information Security, Cyber-attacks, Protection.

INTRODUCTION

The revolution of internet and social media applications resulted in a huge increase in the numbers of internet-connected users worldwide. These statistics provide information on the number of internet users in Saudi Arabia from 2015 to 2023. Saudi Arabia had 21.5 million internet users in 2015; and 31.7 million internet users in 2020. This figure is projected to grow to 35 million internet users in 2023. [3]





FASTFACTS

160,000

The number of daily cyberattacks on the private and public sectors in Saudi Arabia.

$5bn

The expected value of the Kingdom's cybersecurity market by 2022.

SR2.6bn

The amount lost in 2012 due to cybercrime.

45%

The proportion of cyberattacks in the Middle East driven by 'hacktivism.'

23m

The number of internet users in Saudi Arabia in 2018.

73%

The proportion of the Saudi population using WhatsApp, the Kingdom's most popular social network.

SOURCE: GLOBAL FOUNDATION FOR CYBER STUDIES AND RESEARCH

Parallel to the above fact, this increased the number of cyber-attacks on users and companies. Moreover, cybercrime has cost the Kkingdom 2.6 billion Saudi Riyals (SAR) in the last year, according to a report released by Symantec and published by the Ministry of Communications and Information Technology. [2]

According to an IBM report, Saudi Arabia and the United Arab Emirates (UAE) had the second highest average data breach cost at SAR22.4 million ($5.97 million) in 2019 [4]. Saudi Arabia and the UAE also had the highest average number of breached records at 38,800 per incident, compared to a global average of 25,500 records per incident [4]. Saudi Arabia and the UAE took an average of 279 days to identify a data breach and 102 days to contain it, compared to a global average of 206 days to identify and 73 days to contain [4]. Between 2016 and 2018, Saudi Arabia was the sixth most affected country in the world by targeted cyber-attacks. [4]

Cybersecurity Awareness is a formal process for training and educating employees about IT protection, which consists of:

- Programs to educate employees.
- Individual responsibility for company security policies.
- Measures to audit these efforts.

Positive, vigilant and well-trained members of staff are a key part of ensuring that you protect the critical intellectual assets of the organization, such as confidential information, relationships and reputation.

CYBERSECURITY AWARENESS PROGRAM

Cybersecurity awareness should be conducted as an on-going program, to ensure that training and knowledge is not just delivered as an annual activity but used to maintain a high level of security awareness on a daily basis. Moreover, staff should be aware of the importance of applying all the security measures that will lead to the success of the cybersecurity awareness program and help meet the program objectives. To create a successful cybersecurity awareness program, the following are required:

Create a Cybersecurity Awareness Professional team:
The first step in the development of a formal security awareness program is assembling a security awareness team. This team is responsible for the development, delivery, and maintenance of the security awareness program. It is recommended the team be staffed with employees from different areas of the organization, with various responsibilities, who represent a cross-section of the organization. Having a team in place will help ensure the success of the security awareness program through assignment of responsibility for the program.

Determine Roles for Cybersecurity Awareness:
Role-based security awareness provides organizations a reference for training personnel at the appropriate levels based on their job functions. A simplified model groups individuals into three types of roles: All employees, Specialized Roles, and Management. The training can be expanded — and subject areas combined or removed — according to the levels of responsibility and roles defined in the organization.

Establish the Cybersecurity Awareness Communications:
Cybersecurity awareness should be delivered to all employees in multiple ways, including formal training, computer-based training, emails and circulars, memos, notices, bulletins, posters, etc. Moreover, the program should be delivered in a way that fits the overall culture of the organization and has the most impact on personnel.

Define the Cybersecurity Awareness Training Content:
Cybersecurity awareness training content is determined based on the role and the organization's culture. The security awareness team may wish to coordinate with the appropriate organizational units to classify each role to determine the level of respective training required for those specific roles. Regardless of the role, it is recommended that all staff receive basic security awareness training, developed in accordance with organizational policy. Cybersecurity awareness and training materials may be developed in-house, adapted from a professional organization's work, or purchased from a vendor. There are security awareness vendors that provide prepared materials, such as computer-based training (CBT), posters, and newsletters. Furthermore, listed in the reference section [4] are examples of materials that may help in the development of a Cybersecurity Awareness Program.

Below is an example of content that is commonly included in general cybersecurity awareness training. In addition, reference numbers provided for complete awareness materials:

- Organization's cybersecurity awareness policy [5]
- Importance of strong passwords and password controls [6]
- Secure email practices [6]
- Secure practices for working remotely. [6]
- Avoiding malicious software – viruses, spyware, adware, etc. [6]
- Secure browsing practices. [6]
- Mobile device security including BYOD. [6]
- Secure use of social media. [7]
- How to report a potential security incident. [8]
- Protecting against social engineering attacks. [9]
- Physical access
- Phone – caller ID spoofing
- Email – phishing, spear phishing – email address spoofing

Management Leadership Role:
Management leadership support for the Cybersecurity Awareness Program is essential to its successful adoption by staff. Managers are encouraged to:

- Actively encourage personnel to participate and uphold the security awareness principles.
- Model the appropriate security awareness approach to reinforce the learning obtained from the program.
- Include security awareness metrics into management and staff performance reviews.
- Encourage conducting regular awareness sessions for all personnel during staff meetings.
- Encourage compliance reviews for all computer users on a monthly basis.
- Support a recognition program to promote a cybersecurity culture.
- Implement a clear policy defining the consequence for noncompliant users.

Define Metrics to Assess the Cybersecurity Awareness: Metrics can be an effective tool to measure the success of a cybersecurity awareness program and can also provide valuable and current information to enhance the effectiveness of the program. The particular metrics used to measure the success of a security awareness program will vary for each organization, based on considerations, such as size, industry and potential risks.

CONCLUSION

A comprehensive security awareness program sets clear cybersecurity expectations for all employees, and educates users about how to recognize attack vectors, help prevent cyber-related incidents and respond to potential threats. In addition, the program will help all employees recognize threats, see security practices as beneficial enough to make them a habit at work and at home, and feel comfortable reporting potential security issues. Finally, the program will deliver a clear message to all employees that Information Security is everyone’s responsibility.

REFERENCES

[1] IEEE, https://ieeexplore.ieee.org/document/7856687

[2] Ministry of Communications and Information Technology https://www.mcit.gov.sa/en/media-center/news/92474

[3] Statista, https://www.statista.com/statistics/462959/internet-users-saudi-arabia/

[4] National Institute of Standards and Technology (NIST) Special Publication 800-50, Building an Information Technology Security Awareness and Training Program, www.nist.gov

[4] International Standards Organization (ISO) 27002:2013, Information technology -- Security techniques -- Code of practice for information security controls, www.iso.org

[4] International Standards Organization (ISO) 27001:2013, Information technology — Security techniques -- Information security management systems, www.iso.org

[4] COBIT 5 Appendix F.2, Detailed Guidance: Services, Infrastructure and Applications Enabler, Security Awareness, www.isaca.org/cobit

[4] U.S.-Saudi Arabian Business Council - https://us-sabc.org/saudi-arabias-emergence-in-cyber-technology/

[5] Connecticut College - 270 Mohegan Avenue, New London, CT 06320 https://www.conncoll.edu/information-services/ policies/ information-security-awareness-policy/

[6] Infosec https://www.infosecinstitute.com/ https://resources. infosecinstitute. com/ category/enterprise/ securityawareness/ best-tips-for-creating-strong-passwords/

[7] Hootsuite Inc. - https://blog.hootsuite.com/social-media-security-for-business/

[8] University of Michigan - https://spg.umich.edu/policy/601.25

[9] eSecurity Planet - https://www.esecurityplanet.com/ views/ article.php/3908881/9-Best-Defenses-Against-Social-Engineering-Attacks.htm

[10] Global Foundation for Cyber Studies and Research - https://www.gfcyber.org/