International Journal of Engineering & Technology, 7 (2.3) (2018) 54-58

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

A study on cyber-crimes, threats, security and its emerging trends on latest technologies: influence on the Kingdom of Saudi Arabia

Sivaram Rajeyyagari *, Abdullah S. Alotaibi

Computer Science department, Shaqra University, Shaqra, Kingdom of Saudi Arabia
**Corresponding author E-mail: dr.r.sivaram@gmail.com*

Abstract

Now a day the human life penetrated with the technology, like in every moment of life such as shopping or financial transactions and more are using technology in its cyber space. At the same time, it has become very difficult to safe guard the information. The online crime or cybercrime increased along with the heavy usage and development of social media. In case of Saudi Arabia, the cyber-attacks increased because of regional conflicts and low-level awareness about cyber security, and also the perception of Saudi Arabia being extremely wealthy. This paper identifies the importance and impact of cybercrime according to the current situation and Study reports of past activities that have taken place in Saudi Arabia. In addition, described about the cyber security and its emerging trends and latest Technologies along with the policies planned and implemented by the Kingdom of Saudi Arabia. However, the growth of Cyber Crimes becomes proportional to the technological advances. The present paper suggest the solutions to deal with the increasing online crimes in Saudi Arabia with few case studies and have been discussed some innovative suggestions for future cyber security.

Keywords: *Cybercrime; Cyber security; Cyber threats; Saudi Arabia; Social media*.

1. Introduction

As technology and various new trends are coming out day by day and the world is moving towards digital life, it makes necessary for Kingdom of Saudi Arabia to adopt the Information Technology to move along with the world. Technology is playing a major role in every aspect of human life which includes business, education, shopping or banking transactions and more. Almost all the personal information of an individual becomes digitalized, securing this data from the cyber-attacks is a big challenge. As social media has growing the online crimes also increasing. The online crimes or cybercrimes such as hacking of accounts, embezzlement, blackmail, defamation etc. had more impact on the nation's growth.

With the impact of Cybercrimes every year, the companies are losing their billions of money and reputation leading to loss of future business. Computer crime, Pornography or child pornography, cyberbullying, Phishing and selling fakes online are the cybercrimes which are commonly committed with help of computer network technologies or online. The Arab news and some other publications has reported numerous incidents related to cybercrime in the Kingdom of Saudi Arabia, which are mentioned in the following chapters.

Cybercrime and cybersecurity are the separate issues but interconnected. Cyber security is the remediation measure to combat cybercrime. It is necessary to develop new government policy and services to protect internet users. The trends on latest technologies are having huge impact on cyber security.

In the past 12 months the frequent cyber-attacks and consumer cybercrime in the Kingdom of Saudi Arabia has cost SR 2.6 billion [24]. The Saudi Arabian government has established a cybersecurity authority to better protect the country's data, systems and Information Technology networks, and also to improving online security for companies and individuals. "Cybercrime is on the rise across the Middle East and in Saudi Arabia, and protecting against cyber threats is an ongoing management challenge for organizations in Saudi Arabia with the rise of cybercrime across the Middle East [28]".

2. Cyber crimes

Before the computer age also there was criminal offenses, which are now the new phenomenon that can be committed with a computer or smartphone.

2.1. Discussion

The Cybercrimes discussed as below [1], [2].

Computer Crime: Many countries included in their computer crimes laws. Especially in cyber space, one should not perform certain acts without authentication.

Pornography /Child Pornography: The distribution, sharing and obtaining Pornographic material involving children, including images and films using computer technology and internet is a crime.
Cyberbullying: To tease, embarrass, defame, harass, intimidate, or causes to harm to another with the help information and communications technology is one type of cybercrime called Cyberbullying.
Phishing: Phishing is that obtaining personal and financial information fraudulently which causes to get loss from financial institutions like banks. It sometimes involves by asking bank account numbers, credit card numbers, birth dates, Social Security numbers, or various passwords.
Selling fakes online: The business in online becomes the new trend with the availability of internet. Almost anything can be available to sell online to any one at any time. Unfortunately, the fake products also selling in online.

2.2 Motivation behind to commit cyber crimes

a. Ease of access: to break the security system one can steal the pin numbers access codes, retina images etc., used to fool the biometric system and get through out of the firewall [3].
b. Cyber Hoaxes: Involving through Cybercrime by damaging which leads to impact on one's reputation. It's considered as most dangerous. "The involved believe in fighting their cause and wait their goal to be achieved. They are called cyber terrorists [4]".
c. Negligence: There are possibilities of neglecting to take care in protecting the system leads the criminals to damage the computer.
d. Revenge or motivation: The criminals with the lust for making quick money or desire to made loss to the victim they do fraud in transaction or hacks e-comers or e-banking.
e. Poor enforcement in cyber law: many criminals are escaping from the punishments due to poor enforcement in cyber law.
f. Someone intentionally want to be notice through Cyber Crime for publicity or recognition without hurting someone's sentiments [5].

2.3 Cybercrime and Saudi Arabia

According to the ClearSky cyber security firm statistical report on cybercrime attacks, the firm published "the targets of alleged Iranian computer hacking divided by country. Saudi Arabia, at 44 percent, was the most penetrated, followed by Israel (14%), Yemen (11%), Venezuela (8%) and Iraq, United Kingdom, Afghanistan, Kuwait are (3%) [19]".

Some case studies given below to elaborate on the Cyber Crime incidents in the Kingdom of Saudi Arabia.

Case 1: Pornography / Child pornography

i) "The Ministry of Interior (MoI) disclosed here on Thursday that as many as 149 persons were handed over last year to the concerned authorities for browsing or publishing pornographic material related to children". – RIYADH: ABDUL HANNAN TAGO Published on Saturday 14th November 2015.
ii) "The Communications and Information Technology Commission (CITC) has blocked more than 600,000 porn sites over the past two years, and warned that those peddling smut face five-year jail terms and fines of over SR3 million". – JEDDAH: ARAB NEWS Published on Wednesday 16th March 2016.

Case 2: Phishing

"A recent statistic released by the National Cyber Security Center (NCSC) at the Ministry of the Interior stated that the phishing e-mails in Saudi Arabia have exceeded 26 million emails in the past few years. According to NCSC, attackers have deliberately sent fake e-mails (7z. or zip.) containing attached malicious software (Locky Ransomware). NCSC also confirmed that it had sent technical reports, hacking indicators and recommendations to all the entities registered with the NCSC, and advised them to take caution of these phishing e-mails and other hacking techniques". – ARAB NEWS Published on 11 September 2017.

Case 3: selling fakes online

"In a similar move, Saudi Arabia's ministry of trade and investment shut down around 75 accounts on various social media, including Twitter, Facebook, Instagram and Snapchat, for posting thousands of fake good ads". – ARAB NEWS Published on 3rd March 2017.

Case 4: Cyber Bullying

"Novelist and journalist Samar Al-Muqren has won a ruling after filing a complaint against a writer and website owners for online defamation, and is now awaiting the outcome of a second case of cyber bullying". – JEDDAH: Marwa Haddad Published on Monday 4th February 2013.

2.4 Three reasons for cyber-attacks on Saudi Arabia [11]

- The perception of Saudi Arabia being extremely wealthy
- Regional conflicts
- Absence or low level of cyber security awareness and capabilities.

3. Cybersecurity

"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunication systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality [7]."
The importance of Cybersecurity becomes essential along with the growth of internet services and development of information technology. Every nation have to enhance their cyber security to protect their national security and economic growth.
"The legal, technical and institutional challenges posed by the issue of cybersecurity are global and far-reaching, and can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation [8]". The Global Cybersecurity Agenda sets strategic goals on Organizational structures, Legal, Technical and procedural measures, Capacity building and International cooperation [9]. "The fight against cybercrime needs a comprehensive approach. Given that technical measures alone cannot prevent any crime, it is critical that law-enforcement agencies are allowed to investigate and prosecute cybercrime effectively [10]".

3.1 Cyber security trends

There are some trends which have more impact on cyber security are discussed [12], [13], [14], [15].

Web servers: Distribute malicious code or to extract data are the most considerable threat of attacks on web applications. Now a days Cyber criminals are attacking web servers for data stealing by distributing malicious code via legitimate web servers. Now it's become a great need to protect web servers and web applications. And also it's very important to use secured browser while practicing financial transactions where one should not victim of the cybercriminal.

Cloud computing: Because of significant cost savings and efficiencies of cloud computing, the companies are migrating towards the cloud. Operational security planning and well-designed architecture can help organizations to get rid of the risks of cloud computing. Even after developing their own models of cloud services the companies are still facing many issues about their security.

Advanced Persistent Threat and targeted attacks: it is a completely new level of cybercrime ware. The targeted attacks were identified effectively with the network security capabilities like web filtering and Internet Protocol services. Network security must adapt the other security services to detect attacks, because the attackers are growing and use more vague technologies. So that security techniques must be improved to avoid more threats coming in the future.

Mobile Devices and Apps: The extrema development of mobile devices caused the same growth in security risks. Some of the highly targeted malwares intruded through the mobile applications that can steal the important and personal data. Moreover, the devices, which were lost or stolen, are the serious issues to secure the data and information. It extends to include the new technology in cyber security.

IPv6: is a new protocol after IPv4, which is a wholesale replacement in making of very fundamental changes to the protocol for the needs in security policy. To reduce the risk with cybercrime one should switch to IPv6 as soon as possible.

Social Media Networking: The personal cyber threats are growing along with the use of social media growing. Social media become the best tool for the development of business which leads to the threat of attack. To overcome from these risks, companies should use updated technology to prevent leakage, latest technics in network monitoring and log file analysis. There will be more threat of attacks by using social media profiles in the future. To fight with these risks companies should have to use advanced technologies beyond the basic policies and procedures.

Encryption: Messages are encoded using encryption algorithms with encryption key, in such way that hackers cannot read it. And also protects data privacy and its integrity. Encryption of the code will identifies any leakage of information.

Protect systems rather Information: There will be a special importance on protecting information, not just systems. The important information of consumers and businesses are very huge and stored in online that requires advanced security to the data stored systems house. There should be a new strategy to protect the information that to protect the data stored therein.

New Platforms and Devices: these becomes the open door steps to the cybercriminals for new opportunities. The personal computers running Windows have been associated with Security threats. However, the rapid growth in manufacturing new devices with new platforms will likely create new threats.

Hence, some of the trends influences cyber security that turns to its new face in the world.

3.2 Cybersecurity techniques

Access Control and Password Security: The fundamental way of protecting our information is the concept of user name and password. A user must have to prove his identity for attempts to access the network. “The entire field of cybersecurity rests almost completely on identity verification and access control”. Almost there is no security technique without these two functions. “Every other element of security depends on the system identifying the user and validating their permissions to various objects [16]”.

Authentication: the received data should verified that data should be from a trusted and a reliable source without modifications is authentication. Data protection is one of the most significant methods to preventing data from cyber criminals. It provides data privacy, network security, integrity, and identity management to access the data authorized personnel's [17].

Malware scanners: is a mechanism to search malicious code or harmful viruses available in all the files and documents present in the system. Malware includes computer viruses, Trojan horses, ransomware, worms, key loggers, dialers, rootkits, spyware, adware, rogue security software and other malicious programs. “The majority of active malware threats are usually worms or Trojans rather than viruses [18]”.

Firewalls: in general a firewall will be established in between a trusted internal network and untrusted external network. It controls the traffic in between these networks. While controlling the traffic it verifies the incoming and outgoing data blocks are according to the predefined security criteria. Hence the firewalls detects the malware and protects from attacks by cybercriminal.

Anti-virus software: An antivirus software is a must and necessity for every system. It stops unwanted malwares to intrude to our systems. It searches and finds the malwares existing in the systems. Whatever the harmful programs available in the system will be removed by the antivirus software. Therefore, this is very important program for every system to protect the information. Almost antivirus software are with the auto-update option that protects from the latest malwares by updating.

4. Recent cyber-attack targets in Saudi Arabia

According to “Russian cyber-security firm Kaspersky Lab”, for the last one year 60 percent of companies or organizations attacked by the viruses and malwares in the Kingdome of Saudi Arabia [20]. The study report finds that the forty one percent of the organizations expected to prepare for better tools to deal with targeted attacks. [21].

The “OilRig Campaign” named for two waves of attacks in Saudi Arabian Organizations. First attack was in the fall of 2015 and the second attack was in May 2016. The wave attacks primarily focused on financial institutions and Technology institutions. Further, it also aimed to attack on defense industry in Saudi Arabia [22].

In august 2012, “Saudi Aramco” the giant company in petroleum sector undergone with wiper attack, and destroyed data from thirty thousand computers and effected “Rasgas” of Qatar. And another round of wiper attack in 2016 and 2017 destroyed data from different organisations of Saudi Arabia. These wiper attacks called “Shamoon Returned” [23].

Every year Symantec conducts a study on Consumer cybercrime. The study reports found that SR 2.6 Billion cost in the past one year for kingdom of Saudi Arabia. Through this study one can understand that how cybercrime effects consumers, and how to evaluate new technology to secure people. According to this study, many of the adults using online in Saudi Arabia are unaware of how cybercrime have evolved over the year, and how the attacks and viruses act on their computer. In fact, forty percent of the adults are unknown that their computer are with malwares. More than fifty percent of the adults don’t know that there systems are working in clean and free of malwares with good condition [24].

5. Preventive measures to avoid cybercrimes

In reality, it is very hard to manage cybersecurity. “You can’t protect everything equally…we have to find a way to control only what matters,” said Earl Perkins, research vice president, during the “Gartner Security & Risk Management Summit 2017 in National Harbor, Md..” In fact, “security experts should know four things: you can’t fix everything, you can’t make assets fully secure, you can’t know how secure they all are, and you can’t know how secure your digital partners are”.

The five emerging trends in cybersecurity appears for 2018.

1) Skills and organization for cybersecurity continue to change:
2) Cloud security becomes a top priority for many:
3) Shift your focus from protection and prevention
4) Application and data security are maintained at development centers
5) Digital ecosystems drive next generation security

Only with the technical measures cannot prevent Cybercrime, it also required the capacity building, organizational structure and international cooperation along with legal measures.

5.1 Preventive measures taken to avoid cybercrimes in Saudi Arabia.

According to royal decree, National Authority for Cyber Security will linked to the King Salman. Saudi Arabia has set up a new authority for cyber security following a number of attempts to hack government and private-run websites over the past few months. The authority, set up by royal decree, has named the Minister of State Musaed al-Aiban as its chairman, reported state news agency WAM, citing Reuters. The National Authority for Cyber Security will be linked to the Saudi King Salman bin Abdulaziz Al Saud, and has been created to "boost the cyber security of the state, and protect its vital interests, national security and sensitive infrastructure," according to the decree [25].

There is an exclusive digital laboratory in Jeddah managing by the police to fight against cybercrime, because more number of people in the Kingdome are increasing in using the new media and social network. In 2007, 26 March the Royal Degree approved “The Anti-Cybercrime Law”. “The law aims at combating cybercrimes by identifying such crimes and determining their punishments to ensure information security, protection of rights pertaining to the legitimate use of computers and information networks, protection of public interest, morals, common values and protection of the national economy. Cybercrime is on the rise across the Middle East and in Saudi Arabia, and protecting against cyber threats is an ongoing management challenge for organizations in the country [26]”.

5.2 The latest technologies that help us to reduce cyber crime

1. Multi-factor authentication.
2. End to End encryption, Digital Signature: End-to-end encryption.
3. Moving Target Defense
4. Anti-virus/malware software's
5. Artificial Intelligence/ Machine learning
6. Training and awareness program about cyber security, it is very crucial as human errors are mostly involved in most of the cyber-attacks.

5.3 Recommendation

According to the Saudi Anti-Cyber Crime Law the social media users should know and follow their rights and obligations before using the social media. The cybercrime legislations need to be upgraded in line with modern development in the field of Information Technology, especially in KSA. With cyber criminals constantly honing their skills, it is everyone’s responsibility to secure the country. Saudi Arabia has its own respective laws to recognize and punish cybercrimes; there is no developed regulatory framework for data protection in the Kingdom of Saudi Arabia. The country should seek specialist legal advice and employ a cybersecurity consultant if they are unsure of the steps they should take to limit their exposure to cybercrime. KSA should ensure that their internal governance and policies aligned with international standards even where it has not prescribed by domestic legislation.

6. Conclusion

Information Technology development and internet services become the most important aspects in the development of any nation. In this context, Cybersecurity has very prominent role in the area of nation’s security and economic growth. Introducing the new technologies instantaneously according to the unfortunate threats and attacks is very essential in the cybersecurity to prevent the cybercrimes in the nation. Both cybercrime and cybersecurity issues are under one umbrella of interconnected environment. Cybercrimes are proportionally increasing with the advancement of technology. Because of continuously increasing cyber offences with modern technical approaches along with the advancement of technology, we should minimize the cyber-crimes in order to have safe and secure digital life in Kingdom of Saudi Arabia. An extensive approach required to fight against cybercrime. Only technical measures will not help to prevent any crime, along with that investigation and prosecution on cybercrime should made powerful to the law-enforcement agencies.

References

[1] FindLaw, a Thomson Reuters business http://criminal.findlaw.com/criminal-charges/cyber-crimes.html.

[2] Dacey, Raymond & Gallant, Kenneth S. (1997) "Crime control and harassment of the innocent, " Journal of Criminal Justice, Elsevier, vol. 25(4), pages 325-334.

[3] https://www.scribd.com/doc/28079943/Cyber-Crime-in-Banking-sector.

[4] Michael Massourakis & Farahmand Rezvani & Tadashi Yamada (1984) "Occupation, Race, Unemployment and Crime In a Dynamic System, " NBER Working Papers 1256, National Bureau of Economic Research, Inc.

[5] Panu Poutvaara & Mikael Priks (2005) "Violent Groups and Police Tactics: Should Tear Gas Make Crime Preventers Cry?, " CESifo Working Paper Series 1639, CESifo Group Munich.

[6] International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 8 (2014), pp. 835-840 © International Research Publications House http://www. irphouse.com.

[7] Also see: ITU, List of Security-Related Terms and Definitions, available at: www.itu.int/dms_pub/itut/oth/0A/0D/T0A0D00000A0002MSWE.doc.

[8] See in this context: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 14, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[9] For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[10] This publication is available online at: www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

[11] http://alriyadhdaily.com/article/86f4dc5824044704ae0794b8e0d490ae.

[12] A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.

[13] Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole.
[14] Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.
[15] A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.
[16] https://www.cybersecuritymastersdegree.org/access- control/.
[17] Prakash Kuppuswamy, Rashida Banu, Nithya Rekha "Preventing and securing data from cyber crime using new authentication method based on block cipher scheme" , IEEE , 2nd International Conference on Anti-Cyber Crimes (ICACC) on 26-27 March 2017, Abha, Saudi Arabia.
[18] http://www.tnstate.edu/cit/How_to_easily_clean_an_infected_computer.pdf.
[19] Screen capture: www.clearksysec.com.
[20] This finding came in a recent study revealed by Kaspersky Lab during a workshop entitled "Security, Information Technology 2017," which was organized by the Ministry of Interior's National Cyber Security Center (NCSC) in Riyadh.
[21] http://www.arabnews.com/node/1169846/saudi-arabia.
[22] https://researchcenter.paloaltonetworks.com/2016/05/the-oilrig-campaign-attacks-on-saudi-arabian-organizations-deliver-helminth-backdoor.
[23] https://warontherocks.com/2017/07/cyber-attacks-whos-keeping-score/.
[24] http://www.arabnews.com/saudi-arabia/cybercrime-costs-saudi-arabia-sr-26-bn-year.
[25] http://www.arabianbusiness.com/industries/technology/382557-saudi-arabia-sets-up-new-cyber-security-body-as-attacks-increase.
[26] Source: http://www.arabnews.com/news/590406.